UT01: Adopción de pautas de seguridad informática - Amenazas

Nombre: Francisco Jesús García – Uceda Díaz - Albo
Curso: 2º ASIR.

Índice

1a) Amenazas Físicas: Busca en Internet al menos una noticia relacionada con amenazas físicas a sistemas informáticos respecto a:

- Robos, sabotajes, destrucción de sistemas.

Sabotaje informático a clientes BCI: $124 millones llegan a 217 cuentas del Banco Estado.

Un fraude sufrido el 20 de febrero a 25 clientes del Banco de Crédito e Inversiones (BCI) extrajo $124 millones que terminaron en 217 cuentas de BancoEstado. Las estafas oscilan entre el millón 600 mil pesos y 7 millones de pesos por persona.

Así lo consigna un reportaje de BioBioChile. La información proviene de una querella presentada en el Séptimo Juzgado de Garantía de Santiago, por los abogados Francisco Cox y Matías Balmaceda.

Según el documento, los estafadores habrían obtenido las claves privadas de los clientes a través de phishing vía mensajes de texto, un sistema de robo por suplantación de identidad, en el que los ladrones se hacen pasar por funcionarios del banco.

El ataque se produce en días en que el gobierno busca aprobar un proyecto de ley en la cámara de diputados para que sean los bancos y no los clientes quienes asuman los costos producidos por fraude.

- Catástrofes, Incendios.

Un supuesto incendio destapa en Bellreguard una granja de Bitcoins

Un sobrecalentamiento de un local en la playa de Bellreguard ha destapado una granja de criptomonedas, más conocidas como Bitcoins. Un total de 15 equipos informáticos de gran potencia trabajaban a destajo para albergar todo el tráfico que generan este tipo de potentes procesadores. Era tal el calor que desprendían que el propietario de ellos ideó un sistema rudimentario de ventilación con tubos de aluminio que vertían todo el calor a una habitación contigua donde un solo ventilador hacía las tareas de refrigeración.

Un equipo insuficiente a todas luces y que fue el motivo del sobrecalentamiento de paredes y techo. Fue tal la temperatura alcanzada durante varios días que los vecinos del edificio

comenzaron a sospechar. Incluso la vecina del primer piso cuando, ahora en verano andaba descalza por su casa, notaba en los pies la elevada temperatura por lo que dedujeron que algo estaba sucediendo. Ante el aumento incesante de la temperatura en paredes y suelo, decidieron alertar de un posible peligro de incendio y hasta el bajo comercial y el edificio acudieron Bomberos, Policía Local y Guardia Civil. Al entrar descubrieron la granja de Bitcoins por lo que localizaron al propietario y se personó en el local.

Tras inspeccionarlo éste declaró que una persona de Barcelona era la responsable de las operaciones y que se comprometió a abonarle el importe del fluido eléctrico. Cuando supo que la granja había podido triplicar el gasto de luz de todo el edificio el dueño del local apagó los servidores. La investigación trata de dilucidar si hubo defraudación de fluido eléctrico por lo que se incoaron diligencias a la espera de los informes eléctricos. El dueño del local tenía apalabrado el abono de la luz por parte del responsable de la granja que reside en Barcelona.

Normalmente este tipo de servidores se alojan en zonas frías del planeta por lo que no es muy frecuente verlas por la Safor. En zonas como Singapur o China el fluido eléctrico es mucho más caro y el sobrecalentamiento por lo que motiva que busquen puntos en Islandia o Siberia donde la moneda virtual, sus complejas operaciones matemáticas y de seguridad junto con los servidores suelen estar mejor alojados en dichas latitudes.

- Cortes de suministro eléctrico

Un fallo eléctrico tira el sistema informático del Hospital de Móstoles durante cinco horas.

El Hospital Universitario de Móstoles sufrió el pasado viernes pasado un fallo eléctrico que provocó que el sistema informático del centro estuviera caído entre las 16.00 y las 21.00 horas, obligando a cancelar varias pruebas concertadas en Endoscopias y Radiología.

Fuentes del hospital han señalado que el problema sobrevino en torno a las 16.30 horas, cuando tras un breve corte del suministro eléctrico, por un fallo en sus propias instalaciones, el sistema informático con el que funciona el centro sanitario dejó de funcionar y no se pudo recuperar hasta las nueve de la noche.

El apagón digital no afectó a los quirófanos, ya que cuenta con otro sistema eléctrico de urgencia, aunque admiten que el incidente obligó a cancelar 27 pruebas diagnósticas previstas en el servicio de Endoscopias y Radiología.

Aún no se ha localizado el origen de los cortes en el suministro eléctrico que sufre el complejo de forma reiterada, por lo que los técnicos de mantenimiento siguen buscando el punto exacto de la red donde se produce el corte de luz, han añadido fuentes del hospital.

1b) LÓGICAS: Busca en Internet al menos una noticia relacionada con amenazas lógicas respecto a:

- Ataques a un sistema informático

Un virus informático inutiliza un laboratorio médico.

Un virus informático ha inutilizado uno de los mayores laboratorios de analíticas médicas de Cataluña, el Laboratorio de Referencia de Cataluña (LRC). El centro, de titularidad privada pero que presta servicio a varios hospitales de la red pública, sufrió el ataque el pasado viernes. La afectación alcanzó a seis centros sanitarios, que tendrán que procesar toda la actividad que puedan desde sus laboratorios internos. El LRC solo atiende peticiones urgentes.

El ataque provocó la caída de todo el sistema informático del LRC. "La afectación interna del propio LRC ha provocado la imposibilidad de usar el sistema en los centros asistenciales que trabajan habitualmente con este laboratorio", explicó ayer a EL PAÍS un portavoz del Departamento de Salud.

El centro ha aplicado el protocolo de contingencia y ha aislado el programario del laboratorio “para evitar que la infección afectase a los sistemas de información hospitalarios” de los seis centros sanitarios afectados. El Departamento de Salud aseguró que “no se han perdido datos”. Para peticiones urgentes, permanece abierto el circuito alternativo, pero, para las muestras de rutina, los hospitales tendrán que hacerse cargo o derivarlas a Reference Laboratory, un centro que tiene un convenio con el LRC. "Es un laboratorio certificado, de confianza, con suficiente capacidad para asumir la parte de analítica que se le envíe", apuntó el portavoz de Salud.

El virus se llama CryptoLocker y bloquea los archivos del ordenador afectado. Luego, pide una recompensa económica para restaurar los datos. El Centro de Seguridad de la Información (Cesicat) ayuda a las entidades afectadas para eliminar el virus. La Generalitat asegura que el ataque no ha afectado a sus servidores.

- Ciberdelitos

El cibercrimen, un delito con una impunidad de "casi el 100%" en España.

Una impunidad que es "casi del 100%", afirma el jefe del Grupo de Delitos Telemáticos de la Guardia Civil, el teniente coronel Juan Rodríguez de Sotomayor.

De acuerdo con el último informe del Instituto Nacional de Estadística (INE), fue el cuarto delito con más denuncias en España en 2017. Éste refleja que hubo 81.307 delitos cibernéticos ese año y que sólo el 27,2% de éstos fueron esclarecidos. Pero el teniente coronel Rodríguez difiere con esa cifra y asegura que la resolución fue menor dado que "la Fiscalía General del Estado llevó a juicio solo 1.715 casos" y añade no todos fueron de 2017 porque "hubo causas de años anteriores".

Uno de los problemas medulares para combatir su impunidad es la cifra negra. Son los delitos que no se denuncian y que, por lo tanto, no llegan a las autoridades. "Las víctimas se quedan calladas porque les da vergüenza y miedo, se culpan a sí mismas o les humilla la situación", explica Diego Quintana, el abogado penal de la asociación contra el cibercrimen Stop Haters. En el cibercrimen la cifra negra es particularmente alta y significa que la impunidad es aún mayor que la que se ve reflejada en las estadísticas. El teniente coronel Rodríguez asegura que como mínimo es de un 30% y como máximo podría ser de un 50%, es decir, la mitad de los crímenes cibernéticos no llegan a las autoridades y no se investigan.

Otra característica son los servicios que facilitan la ejecución de los delitos cibernéticos, como lo sería la venta de bases de datos de información o plataformas prediseñadas para llevar a cabo estafas, conocidos como crimen como servicio. Sobre este tema, el policía investigador y doctor en criminología Abel González afirma que, si bien no todas las industrias criminales se han trasladado al plano virtual, la mayoría utilizan sus servicios: "La nueva tendencia es el blanqueo de capitales, conocido como ciber blanqueo. Son organizaciones que ofrecen lavado de dinero a grupos criminales, sobre todo al narcotráfico. Se realiza a través de videojuegos como Fornite. Compran la moneda virtual que se usa en el videojuego, los V-Bucks, con dinero negro y se lo venden a los jugadores por un precio más barato en el internet profundo.

Uno de los retos para combatir este tipo de delitos es el lugar donde se llevan a cabo: el ciberespacio. Un ámbito intangible y sin fronteras donde navegan millones de usuarios. Lo cual supone que su alcance es mucho mayor que el del crimen normal.

Los expertos afirman que en España la mayoría de los ciberdelitos son ejecutados por criminales que se encuentran en cuatro países: Rusia, Ucrania, Rumanía y Nigeria.

- Ciberfraudes

Destapan uno de los mayores casos de ciberfraude en Estados Unidos.

Un canadiense y dos ciudadanos vietnamitas han sido acusados de ejecutar uno de los mayores casos de ciberfraude masivo. Se les acusa de robar 1.000 millones de direcciones de correo electrónico para después bombardearlas con spam con información de software pirata.

El Departamento de Justicia de Estados Unidos ha señalado que en los documentos presentados en la corte no se identificaron las compañías que alojaban estas cuentas vulneradas. La Justicia ha descrito este hackeo como «uno de los mayores» detectados en la historia de los Estados Unidos.

Viet Quoc Nguyen, de 28 años, está acusado de piratear al menos ocho proveedores de servicios de correo electrónico entre febrero de 2009 y junio de 2012. El Gobierno alega que Nguyen y Giang Hoang Vu, de 25 años, ambos ciudadanos vietnamitas, utilizaron las direcciones de correo electrónico robado para identificar decenas de millones de personas en una campaña de spam.

Con este spam ofrecían la venta de software falso bajo el nombre de Adobe System. Los dos vietnamitas residían en Holanda. Hoang Vu, fue extraditado a los Estados Unidos en marzo del año pasado y se declaró culpable en el cargo de conspiración para cometer fraude informático. Nguyen sigue prófugo de la justicia.

El tercer acusado es el canadiense David-Manuel Santos Da Silva, de 33 años, que se enfrenta al cargo de conspiración para realizar lavado de dinero. Santos Da Silva es copropietario de una empresa llamada 21 Celsius Inc, con la que Nguyen y Vu habían llegado a un acuerdo para lavar el dinero proveniente del fraude del spam. [Así se realizó el robo informático del siglo]

Según los documentos presentado en la corte, Da Silva y Nguyen recibieron aproximadamente dos millones de dólares en comisiones por la venta del software, una copia pirata de Adobe Reader. Da Silva fue detenido en un aeropuerto de Florida el mes pasado.

- Vulnerabilidades y Amenazas

EternalBlue no deja de infectar equipos, pese a que puedes evitarlo fácilmente

EternalBlue comenzó a ser un problema a inicios del año 2017. Es un exploit que afecta a una vulnerabilidad a la hora de implementar el protocolo SMB de Microsoft. Esto significa que un equipo que no ha sido parcheado es vulnerable a este problema y, en definitiva, ser una amenaza para los usuarios.

A partir de esta vulnerabilidad, a partir de EternalBlue, surgieron numerosas amenazas. Podemos mencionar algunos ransomware como WannaCry y también botnets. Una de las últimas es la botnet Smominru. En el último mes ha infectado a más de 90.000 equipos con Windows aprovechando el exploit de EternalBlue.

Básicamente lo que hacen para lograr explotar esta vulnerabilidad y desplegar amenazas como la que mencionamos de la botnet Smominru es basarse en sistemas que no han sido actualizados. Aún hoy en día hay muchos equipos en todo el mundo que no han corregido esta vulnerabilidad y por tanto son vulnerables a sufrir ataques.

Resulta sencillo protegerse de EternalBlue y sus derivados. Son muchas las variedades de malware y amenazas de seguridad que hay por la red. Muchos tipos de ataques que pueden afectar a nuestra seguridad y privacidad.

Actualizar el equipo, lo más importante:

Sin duda lo más importante para protegernos de EternalBlue es actualizar nuestro equipo Windows. Se basa en una vulnerabilidad que fue corregida hace tiempo por Microsoft. El problema es que muchos usuarios aún mantienen su equipo obsoleto y esto significa que siguen siendo vulnerables. Lo principal que tenemos que hacer es actualizar Windows si no lo hemos hecho. Hay que asegurarse siempre de tener los últimos parches de seguridad instalados.