STUXNET | LA PRIMERA CIBERARMA DE LA HISTORIA

en el año 2010 el mundo conoció la existencia de un programa informático malicioso que por primera vez en la historia iba mucho más allá de de negar servicios robar información u obtener dinero un programa informático que llegó a provocar daños materiales en instalaciones físicas equivalentes a las de un bombardeo aéreo se dio a conocer la primera ciber arma en el mes de marzo del 2010 los operadores de la planta de enriquecimiento de uranio en natanz irán se sobresaltaron al darse cuenta de que los rotores de varias cascadas de centrifugadoras a gas habían comenzado misteriosamente a experimentar una aceleración y una desaceleración continúa sin control provocando que centenares de ellas presentaran fallas en un muy corto periodo de tiempo debiendo dejarlas en consecuencia fuera de servicio cuál era la consecuencia de todo esto que la producción de uranio estaba disminuyendo de forma considerada no era la primera vez que pasaba un par de meses atrás ya había sucedido algo parecido y a finales del 2009 también llegaron a tener ciertos problemas de sobrepresión que habían dejado inservibles varias decenas de centrífugas claro los ingenieros operadores y mantenedores estaban flipando nos decían pero qué cojones están mal hechas están estas centrifugadoras de mierda que tenemos o qué demonios está pasando que acaso este un sabotaje o estamos teniendo un problema en la planta llegó a ser tal la incertidumbre que les había llegado el momento por tanto de analizar a fondo todo el problema y de verificar todos los equipos involucrados porque desde luego por alguna razón hasta ese entonces desconocida se habían llegado a destruir más de un millar de centrífugas hoy vamos a estar hablando de stuxnet la primera arma digital de la historia me gustaría que tomase asiento porque desde luego la historia de hoy está para vérselas mientras comes palomitas va a estar muy interesante pero para más interesante nuestro sponsor de hoy hayes fan es una página que ofrece claves de software oem baratas y legales las cuales son 100% oficiales y que pueden ser activadas totalmente en línea disponen de un servicio de atención al cliente 24/7 y un servicio postventa de por vida una excelente oportunidad para renovar el sistema operativo y lograr una mejora en el rendimiento y la seguridad como podéis ver en la página web pues disponen de múltiples productos a adquirir desde windows 10 hasta windows 11 cuentan también con productos de microsoft office desde el 2000 6 hasta el 2019 y 2021 con licencias disponibles desde para un único ordenador hasta para 5 equipos contamos también con la sección de spam del producto donde en caso de que te quieras pidieron windows 10 y a la vez la suite el office 2010 y 9 para bono tienes un precio un poco más razonable más asequible y por último una sección de computer tools de herramientas de ordenador las cuales pues igual te interesan pillar y por él las tinas disponibles pese a que el precio ya es asequible de por si puedes utilizar el código de cupón v de 50 para obtener un 50% de descuento en la serie windows y por otro lado puedes utilizar el código de cupón vdd 62 para obtener un 62 por ciento de descuento en los productos de microsoft office y también en los bam del producto yo por ejemplo que lleva haciendo ahora pues me voy a pillar un windows 10 pero así que voy a añadir esto al carrito y bueno voy a usar el cupón v de 50 para obtener un 50% de descuento y ahí está ahora yo puedo pagar con paypal o con tarjeta de crédito muchas gracias a cage fan por patrocinar este vídeo y ahora continuemos con el vídeo de hoy aunque los iraníes en ese momento no lo sabían estaban siendo víctimas de stuxnet el primer malware informático que conseguía ocasionar daños físicos en una instalación industrial era la primera vez que un programa informático estaba siendo usado como

armamento consiguiendo a través de 500 kilobytes de líneas de código almacenadas inicialmente en un pendrive un efecto similar a un bombardeo aéreo de precisión la primera ciber arma había entrado en acción' hablemos del uranio primeramente y de su enriquecimiento anteriormente se había estado prestando atención hablamos de una planta de enriquecimiento de uranio en natanz bien pues qué tiene que ver el uranio con toda esta historia bueno pues mucho la razón del uso de stuxnet contra iran está directamente relacionada con el elemento químico uranio y su posible uso en la construcción de bombas atómicas digamos que en su estado natural el uranio cuenta con dos isótopos los isótopos para los que no sepan lo que es son los átomos de un mismo elemento cuyos núcleos tienen una cantidad diferente de neutrones pues en su estado natural el uranio cuenta con dos isótopos por un lado el uranio 238 se encuentra concentrado al 99% y el uranio 235 con el 0 7% restante siendo este último el único fisible es decir que puede ser dividido en dos o tres fragmentos y que en consecuencia podría ocasionar una reacción nuclear en cadena esto siempre y cuando obviamente contenga la masa crítica y la concentración necesaria para desencadenar la dependiendo del grado de enriquecimiento del uranio se pueden conseguir cosas por ejemplo enriqueciendo el uranio se puede llegar a producir energía eléctrica con el denominador low en rage el uranio entre el 3% y el 20% de concentración de uranio 235 necesitaríamos para conseguir esto por otro lado lo más crítico en caso de querer tensar la un poco más fuerte podríamos enriquecer lo sobre el 90% con el denominado height en raid set uranio pudiendo producir por ejemplo pues una bomba atómica como entra en juego stuxnet en todo esto bueno pues prepararos porque para que veáis semejante obra maestra a lo largo de la historia se ha llegado a determinar que han habido variantes de stuxnet partiendo de unas menos agresivas desde principios del 2007 no desde el 2009 como se creía anterior y hasta otras ciertamente más agresivas según la investigación del acné que no voy a apoyar mucho en ella os dejaré el manual en pdf en la descripción de este vídeo el propósito principal de stuxnet era retrasar el programa nuclear iraní la central iraní usa centrifugadoras para enriquecer el uranio hasta ahí bien bien pues el modelo que empleaban era y no sé hasta qué punto lo sigue siendo a día de hoy el modelo era una originalmente desarrollado en europa el año 60 el cual fue robado por a cook aunque este señor maravilloso que vemos por aquí un traficante de secretos nucleares que lo entregó a irán en los años 80 claro los ingenieros iraníes se ve que no lograron dominar la complejidad del sistema por completo y en consecuencia pues no lo pudieron poner a funcionar a pleno rendimiento sabe que era pues ciertamente complicado el manejar este cacharro sin embargo sí que lograron producir esas centrifugadoras a escala industrial de tal forma que podían sustituirlas más rápido de lo que se rompía y es que aislado que no lograron dominar su complejidad que esto podría ser considerado un problema otro de los problemas de estas centrifugadoras que fabricaba iram era que no eran muy robots me explico se rompían con relativa facilidad así que bueno tuvieron que idear un sistema que les permitían aislar las y reemplazarlas todo esto de la mano de ingeniero sin embargo para poder hacer esto habían que parar las centrifugadoras de cara a la siguiente etapa a la que hubiese fallado a qué me refiero con esto de la siguiente etapa en su planta de natanz los iraníes habían implementado un proceso de enriquecimiento de uranio con centrífugas a gas empleando varias etapas en un proceso de cascada en forma que la salida de una etapa era la entrada de la siguiente en las cuales el uranio ha pasado por varios grupos de centrífuga que iban progresivamente enriqueciendo lo claro espera un sistema de protección este sistema digamos que se implementó con la idea en mente de poder aislar centrífugas individualmente cuando presentaran inconvenientes e incluso permitir cambiarlas sin detener el proceso productivo donde

está lo interesante al parar estas centrifugadoras la presión subida y en consecuencia los rotores sufrían daño un rotor para el que no sepa lo que es es algo como esto vale consideremos lo como un componente que gira en una máquina eléctrica o se acabó qué pasa si la presión supera un límite máximo la instalación podría llegar a explotar en consecuencia por lo que diseñar válvulas que liberasen la presión en caso de que subiera por encima de un límite digamos como para medio tenerlo controlado todas estas válvulas por tanto eran el primer punto débil del diseño de la central de natanz por tanto se aparece a pensar si nos ponemos del lado de la mente del atacante ya teníamos una vía potencial de digamos vulnerar todo este sistema para retrasar e incluso ocasionar daños en el programa nuclear iraní a fin de cuentas según representa el manual pues éste era uno de los principales objetivos no sea retrasar el programa nuclear iraní con esto en mente otro punto débil eran los propios rotores de la centrifugadora el diseño del aire uno era súper crítico dado que para llegar a las velocidades normales de operación que eran 63 mil revoluciones por minuto los rotores pasaban por varias velocidades críticas o armónicos a estas velocidades se produce un fenómeno de resonancia que hace vibrar los rotores y claro digamos que esa vibración no es que le sienten muy bien a los rotores estas velocidades por tanto digamos que serían el segundo punto débil de la central entonces bien si nos paramos a pensar ya como atacantes tendríamos vías potenciales de atacar o bueno más que atacar pues en lo que enfocar la atención y ahora en base a esto que ya entendemos el contexto pues vamos a ver las diferentes versiones de stuxnet bien pues veamos la primera versión de stuxnet una versión agresiva pero ciertamente discreta la primera versión de stuxnet tenía como objetivo los controladores industriales siemens s 7 417 los encargados de controlar las válvulas y sensores de presión de la centrifugadora en aquel entonces stuxnet venía en formato de un archivo de configuración para el software de siemens por fuera parecía normal pero por detrás explotaba algunos fallos para poder ejecutar sus acciones la infección de estos controladores digamos que era ciertamente poco glamurosa alguien debía abrir manualmente ese archivo de configuración ya fuerza a través de un usb o llevándolo guardado en uno de los portátiles que se usaban para configurar los sistemas claro cabe destacar que en aquel entonces stuxnet la primera versión pues digamos que no tenía formas de auto propagarse ya más adelante pues en otras versiones sí que había en métodos de auto propagación por lo cual la cosa se pensaba mucho nada bueno fijaros qué locura cuando el archivo malicioso se cargaba se saltaba el código propio de la ejecución y tomaba el control del sistema pero de forma muy discreta reemplazaba las funciones del sistema que permitían al código acceder a las lecturas de los sensores y después dejaba que todo se ejecutarse normalmente como si no pasara nada sin embargo y ahí es donde entra en juego el stuxnet cuando se daban ciertas condiciones stuxnet entraba en acción' grababa 21 segundos de lecturas de los sensores y entonces los reproducía en bucle más concretamente para los curiosos sobre escribía las regiones de memoria en las que se almacenaban los datos leídos con los que había grabado de esta forma cuando el sistema de control es cada en otro ordenador externo al controlador siemens pidiese a las lecturas el controlador devolvería las lecturas reproducidas de stuxnet y ni los ingenieros ni los sistemas automáticos pues verían nada anormal digamos que era como una forma de evitar hacer saltar las alertas una vez que stuxnet el muy guarro había echado el telón se ponía a trabajar aislando etapas de las centrifugadoras de tal forma que la presión del sistema comenzaba a subir claro cuál era la idea que en este momento supuestamente las válvulas de escape deberían actuar y dejar salir el exceso de presión pues bueno no lo hacía estas válvulas cabe destacar que cuentan con sensores de presión analógicos para traducir esa señal a una digital que pueda entender un ordenador

tienen que calibrar se manualmente bueno pues stuxnet el muy guarro los descalibrada de tal forma que las válvulas no detectaban presiones anormalmente altas y por lo tanto pues no sabrían la presión dentro del sistema empezaba a subir hasta que stuxnet decidía parar el ataque y llegamos que parar el ataque no querían ocasionar una bomba atómica una catástrofe no no del todo los creadores de stuxnet podría haber destrozado totalmente las instalaciones nucleares de natanz sin embargo no lo hicieron porque había otra forma mejor de conseguir sus propósitos retrasar el programa nuclear iraní que es lo que les interesaba ya no paramos a pensar que un fallo catastrófico realmente en la central habría llevado los ingenieros a analizar exhaustivamente qué había pasado y probablemente habrían detectado y corregido el problema esto junto a la capacidad iraní de producir centrifugadoras digamos que habría supuesto un retraso no muy problemático no tan significativo stuxnet simplemente modificaba periódicamente las condiciones de la centrifugadora causando principalmente mucho más estrés sobre los rotores provocando fallos y reemplazos más frecuentes de esta forma lograban tener a los ingenieros frustrados con esta cara buscando que provocaba una tasa de fallos tan grande en los sistemas obviamente no buscaban malware ellos buscaban fallos en el diseño o en la construcción ellos no sabían que estaban siendo atacados ni que había un gusano por ahí que se había colado que la estaba liando parda vamos en resumen que la primera versión de stuxnet estaba hecha para tocar la pinga vale bien pues qué novedades trae la segunda versión de stuxnet frente a todo lo que hemos comentado la anr menciona en el análisis que mientras la primera versión de stuxnet parece hecha por un grupo de expertos industriales y programadores en la segunda se aprecia la influencia de gente muy relacionada con el mundo de la seguridad los sospechosos principales se llegó a detectar en su momento que fueron ingenieros de prepárate la enee sea la primera diferencia de la versión 2 de stuxnet frente a las anteriores es el método de propagación parece ser que en su momento pues perdieron el acceso directo a los sistemas de la central así que claro tuvieron que inventar otro método para infiltrarse usando cuatro vulnerabilidades cero de hay que recordar que son vulnerabilidades no descubiertas hasta la fecha stuxnet infectaba unidades usb para transmitirse de un ordenador a otro además usaba una vulnerabilidad en el sistema rpc de windows para infectar a los ordenadores de una misma red privada y bueno por si esas cuatro vulnerabilidades se lo dijo aparecen pocas stuxnet había sido firmado también con certificados digitales robados de esta forma windows lo detecta va como un driver legítimo y confiable y no notifica al usuario de la infección una jugada y maestra muy bien así me gusta stuxnet se movía por tanto ahora en redes privadas y confiables pero seguía habiendo un problema como llevarlo a la central de nata desde luego pasar todos los sistemas de seguridad no es que fuera fácil pero había otro punto débil contratistas externos que trabajaban en la central infectando uno de sus ordenadores menos protegidos stuxnet acabaría entrando más tarde o temprano en los sistemas de natanz claro paramos a pensar no sólo haría falta que ese contratista conectará su portátil o su usb a un ordenador de la central y entonces ya sería cuestión de tiempo que stuxnet llegará a su objetivo que a fin de cuentas eran los controladores siemens estos controladores se encargaban de los rotores no el segundo punto débil que habíamos detectado y discutido de antes cómo operaba esta versión más moderna de stuxnet más o menos una vez al mes stuxnet tomado el control del sistema que se encargaba de gestionar la velocidad de los rotores lo que hacía el muy sinvergüenza era aumentar la velocidad de rotación de las centrífugas de una velocidad normal de 63 mil revoluciones por minuto a 84 mil revoluciones por minuto para después de tenerlas casi completamente a 120 revoluciones por minuto generando con el semejante frenazo una alta carga

de trabajo a los materiales de las centrífugas y ocasionando en consecuencia una degradación de la eficiencia del proceso de enriquecimiento del uranio recordad como comentamos antes para llegar ahí los rotores pasan por diferentes velocidades críticas generando ese fenómeno de resonancia que hacen que vibren y reduciendo en consecuencia su vida útil porque a medida que vibran pues se deteriora en este caso cabe destacar que stuxnet no necesitaba falsificar la lectura de velocidad de los rotores como normalmente los rotores operan a un número constante de revoluciones por minuto no hacía falta reproducir lecturas anteriores el malware simplemente muy ingenioso se encargaba de que no se ejecutase el código que actualice el memoria las lecturas de velocidad como el software de control escala obtenía los valores de las lecturas de la memoria y no comunicándose con los sensores del rotor pues siempre obtendría la misma lectura la de la última vez que se había actualizado por lo tanto todo parecería bastante normal a los ojos de cualquier sistema de monitorización automático o humano la segunda versión de stuxnet cabe decir que real no es que fuera muy sigilosa como algunos ya se habrá imaginado el llevar varios cientos de rotores de 63 mil revoluciones por minuto a 120 revoluciones por minuto no es algo que pase desapercibido si estamos atentos al ruido que hace sin embargo buena jugada los ingenieros iraníes llevaban siempre en todo momento cascos protectores siempre y no oían los cambios de velocidad además stuxnet se comunicaba a través de la red para sincronizar los ataques en varios controladores al mismo tiempo lo que generaba un tráfico sospechoso y fácilmente detectable si se estuviese monitorizando todo esto te hace pensar que ya no es que estuvieran tan preocupados en que se les detectara no era como digamos una prioridad el que les detectara más bien yo creo que estaban tratando de ver hasta dónde podían llegar con esta creación estaban experimentando con lo que ya sabían que sería el primer paso de la ciberguerra stuxnet se podría considerar la primera ciber arma de hecho fueron pioneros en este mundo yo creo que por un lado nos muestran lo vulnerables que pueden llegar a ser los sistemas industriales los fallos de los que se aprovecharon para introducirse en los controladores siemens son fallos de diseño de software no los simples books y por lo tanto es más difícil que se corrijan con un parche aplicado rápidamente ya sabéis que esto tarda pues su tiempo por otra parte creo que también nos muestra el grave problema de seguridad que tenemos en cuanto a el control de acceso físico a las instalaciones oa estos sistemas la segunda versión uso varias vulnerabilidades serveis en windows pero la primera se introdujo manualmente y sin tanta virguería informática desde luego hay muchos puntos de acceso a estos sistemas vulnerables y es difícil tenerlos todos controlados pero cabrón y todo esto ha ocurrido en una central nuclear osea imaginando que puede ocurrir en infraestructuras civiles mucho menos protegidas yo considero que este malware nos demostró a todos que las ciberarmas existen y que pueden llegar a producir efectos militares similares al armamento convencional desde luego pone los pelos de punta y deja uno como ciertamente preocupado pero nos preocupe es que el título xavi está aquí para parar la ciberguerra vale yo me encargo y lo voy a hacer de la siguiente forma as t bueno espero que haya resultado interesante toda esta historia me gustaría saber vuestra opinión en los comentarios qué os ha parecido consideréis que las ciberarmas ya existen incluso mucho antes del 2007 sólo que no lo sabemos o qué opináis bueno cualquier historia que veáis que digamos que sea factible comentarla o narrar la para que aprendamos todos cosas nuevas y tal dejar un comentario y decido y editó sabes pues habla de esta historia o de este señor que tiene una historia vamos espeluznante veréis qué son ataques sofisticados este que hemos visto o creéis que está hecho por un lander de 15 años y bueno poco más la verdad que ha pasado bastante poco tiempo desde el anterior vídeo o sea que he cumplido este mes hemos

tenido dos vídeos es un espectáculo vamos mejorando bueno recordar que tenemos una comunidad en disco que ya ha llegado a los 40 mil miembros un espectáculo agradecería que es un gerais que por ahí si tenéis dudas de ciberseguridad lo que corresponde a la gente se vuelca un montón en echar un cable y bueno cualquier cosa recordad que siempre todos los días me podéis encontrar a las 9 horas de españa peninsular en tu espalda y estamos siempre todos los días rompiendo la mamona dándole caña y al hakim a nivel técnico si queréis ver a tito sabe con tecnicismos maniobrando y tal así estamos creando máquinas de una plataforma y pasándolo muy bien y poco más no olvidéis de dejar un buen line en el vídeo para motivarme a hacer más vídeos y bueno espero que los exámenes os hayan salido bastante bien y ya había suspendido pues bueno seguir suspendido lo que todo haber estudiado ahora gracias por estar en este vídeo acompañándonos y nos vemos en el siguiente vídeo chao e