BlackCat Ransomware aumenta la apuesta tras la interrupción del FBI

diciembre 19, 202335 Comentarios

La Oficina Federal de Investigaciones (FBI) de Estados Unidos reveló hoy que se infiltró en la segunda banda de ransomware más prolífica del mundo, un grupo criminal con sede en Rusia conocido como ALPHV y BlackCat. El FBI dijo que se apoderó del sitio web oscuro de la pandilla y lanzó una herramienta de descifrado que cientos de empresas víctimas pueden utilizar para recuperar sistemas. Mientras tanto, BlackCat respondió "desmantelando" brevemente su sitio de la red oscura con un mensaje que prometía comisiones del 90 por ciento para los afiliados que continuaran trabajando con el grupo criminal y temporada abierta para todo, desde hospitales hasta plantas de energía nuclear.

Una versión ligeramente modificada del aviso de incautación del FBI en el sitio de la red oscura BlackCat (se agregaron mayúsculas de Papá Noel).

Los rumores sobre una posible acción policial contra BlackCat llegaron en la primera semana de diciembre, después de que el sitio de la red oscura del grupo de ransomware se desconectara y permaneciera indisponible durante aproximadamente cinco días. BlackCat finalmente logró volver a poner su sitio en línea, culpando de la interrupción al mal funcionamiento del equipo.

Pero hoy, el sitio web de BlackCat fue reemplazado por un aviso de incautación del FBI, mientras que los fiscales federales de Florida publicaron una orden de registro que explica cómo los agentes del FBI pudieron obtener acceso e interrumpir las operaciones del grupo.

Una declaración sobre la operación del Departamento de Justicia de Estados Unidos dice que el FBI desarrolló una herramienta de descifrado que permitió a las oficinas de campo y socios de la agencia en todo el mundo ofrecer a más de 500 víctimas afectadas la posibilidad de restaurar sus sistemas.

"Con una herramienta de descifrado proporcionada por el FBI a cientos de víctimas de ransomware en todo el mundo, las empresas y las escuelas pudieron reabrir, y los servicios de atención médica y de emergencia pudieron volver a estar en línea", dijo la Fiscal General Adjunta Lisa O. Monaco. "Seguiremos dando prioridad a las perturbaciones y colocando a las víctimas en el centro de nuestra estrategia para desmantelar el ecosistema que alimenta el ciberdelito".

El Departamento de Justicia informa que desde la formación de BlackCat hace aproximadamente 18 meses, el grupo criminal ha atacado las redes informáticas de más de 1.000 organizaciones de víctimas. Los ataques BlackCat suelen implicar cifrado y robo de datos; Si las víctimas se niegan a pagar el rescate, los atacantes suelen publicar los datos robados en un sitio de la red oscura vinculado a BlackCat.

BlackCat se formó mediante la contratación de operadores de varias organizaciones de ransomware disueltas o competidoras, incluidas REvil, BlackMatter y DarkSide. Este último grupo fue responsable del ataque al Colonial Pipeline en mayo de 2021, que provocó escasez de combustible y aumentos de precios en todo el país.

Como muchas otras operaciones de ransomware, BlackCat opera bajo el modelo de "ransomware como servicio", donde equipos de desarrolladores mantienen y actualizan el código del ransomware, así como toda su infraestructura de soporte. Los afiliados están incentivados a atacar objetivos de alto valor porque generalmente obtienen entre el 60 y el 80 por ciento de los pagos, y el resto va a parar a los delincuentes que ejecutan la operación de ransomware.

BlackCat pudo recuperar brevemente el control de su servidor darknet hoy. No mucho después de que se publicara el aviso de incautación del FBI, la página de inicio fue "desconectada" y modernizada con una declaración sobre el incidente desde la perspectiva del grupo de ransomware. Continuar leyendo →

Diez años después, nuevas pistas sobre el incumplimiento del objetivo

diciembre 14, 202325 Comentarios

El 18 de diciembre de 2013, KrebsOnSecurity dio la noticia de que el gigante minorista estadounidense Target estaba luchando contra una intrusión informática de amplio alcance que comprometió más de 40 millones de tarjetas de pago de clientes durante el mes anterior. El malware utilizado en la infracción de Target incluía la cadena de texto "Rescator", que también fue el nombre elegido por el ciberdelincuente que vendía todas las tarjetas robadas a los clientes de Target. Diez años después, KrebsOnSecurity ha descubierto nuevas pistas sobre la identidad real de Rescator.

Rescator, anunciando un nuevo lote de tarjetas robadas en una infracción de 2014 en P.F. De Chang.

Poco después de publicar la historia de Target, KrebsOnSecurity informó que Rescator parecía ser un hacker de Ucrania. Los esfuerzos para confirmar mi informe con ese individuo terminaron cuando se negaron a responder preguntas y después de que yo me negué a aceptar un soborno de 10.000 dólares para no publicar mi historia.

Ese informe se basó en pistas de uno de los primeros foros rusos sobre delitos cibernéticos en el que un hacker llamado Rescator, usando la misma imagen de perfil que Rescator era conocido por usar en otros foros, afirmó haber sido conocido originalmente como "Helkern", el apodo elegido por el administrador de un foro sobre ciberdelincuencia llamado Darklife.

KrebsOnSecurity comenzó a revisar la investigación sobre la identidad real de Rescator en 2018, después de que el Departamento de Justicia de Estados Unidos revelara una acusación que nombraba a otro hombre ucraniano como Helkern.

Puede resultar útil recapitular primero por qué se cree que Rescator está tan estrechamente relacionado con la infracción de Target. Para empezar, se encontró la cadena de texto "Rescator" en algunos de los programas maliciosos utilizados en la infracción de Target. Los investigadores determinarían más tarde que una variante del malware utilizado en el Ta

La violación de rget se utilizó en 2014 para robar 56 millones de tarjetas de pago de clientes de Home Depot. Y una vez más, las tarjetas robadas en la vulneración de Home Depot se vendieron exclusivamente en las tiendas de Rescator.

El 25 de noviembre de 2013, dos días antes de que Target dijera que la violación comenzara oficialmente, se podía ver a Rescator en mensajes instantáneos contratando a otro miembro del foro para verificar 400.000 tarjetas de pago que, según Rescator, habían sido recientemente robadas.

En la primera semana de diciembre de 2013, la tienda en línea de Rescator, rescator[.]la, vendía más de seis millones de registros de tarjetas de pago robadas a clientes de Target. Antes de la violación de Target, Rescator había vendido en su mayoría lotes mucho más pequeños de tarjetas robadas y datos de identidad, y el sitio web permitía a los ciberdelincuentes automatizar el envío de transferencias bancarias fraudulentas a mulas de dinero con sede en Lviv, Ucrania.

Finalmente, existe cierto honor entre los ladrones, y en el mercado de datos de tarjetas de pago robadas se considera de mala educación anunciar un lote de tarjetas como “suyo” si simplemente está revendendo tarjetas que le vendió un proveedor de tarjetas externo o ladrón. Cuando los vendedores serios de tiendas de tarjetas de pago robadas desean comunicar que un lote de

tarjetas es exclusivamente obra suya o de su equipo inmediato, se refieren a ello como “nuestra base”. Y Rescator fue bastante claro en sus anuncios que estos millones de tarjetas fueron obtenidas de primera mano.

ESCENA RETROSPECTIVA

Las nuevas pistas sobre la identidad de Rescator salieron a la luz cuando revisé el informe sobre una historia de abril de 2013 aquí que identificó al autor del troyano OSX Flashback, una de las primeras variedades de malware para Mac que se extendió rápidamente a más de 650.000 computadoras Mac en todo el mundo en 2012.

Esa historia sobre el autor de Flashback fue posible porque una fuente había obtenido una cookie de autenticación del navegador web para un miembro fundador de un foro ruso sobre cibercrimen llamado BlackSEO. Cualquiera que posea esa cookie podría navegar por el foro BlackSEO solo por invitación y leer los mensajes privados del usuario sin tener que iniciar sesión.

El miembro VIP de BlackSEO.com, "Mavook", le dice al administrador del foro Ika en un mensaje privado que él es el autor de Flashback.

El propietario legítimo de esa cookie de usuario de BlackSEO se llamaba Ika, y los mensajes privados de Ika en el foro mostraban que era amigo cercano del autor de Flashback. En ese momento, Ika también era el administrador de Pustota[.]pw, un foro ruso estrechamente vigilado que contaba entre sus miembros con algunos de los spammers y creadores de malware más exitosos y establecidos del mundo.

Durante muchos años, Ika ocupó un puesto clave en uno de los proveedores de servicios de Internet más grandes de Rusia, y su (mayormente brillante) reputación como proveedor confiable de alojamiento web para la comunidad de ciberdelincuentes rusa le brindó un conocimiento enciclopédico sobre casi todos los actores importantes en esa escena. En el momento.

La historia sobre el autor de Flashback presentaba capturas de pantalla redactadas que fueron tomadas de la cuenta BlackSEO de Ika (ver imagen arriba). El día después de que se publicó esa historia, Ika publicó un discurso de despedida a sus compañeros, expresando conmoción y desconcierto por el aparente compromiso de su cuenta BlackSEO.

En una extensa publicación del 4 de abril de 2013 titulada “NO ENTIENDO NADA”, Ika dijo a los miembros del foro de Pustota que estaba tan asustado por los acontecimientos recientes que cerraría el foro y abandonaría por completo el negocio del cibercrimen. Ika contó cómo la historia del Flashback había llegado la misma semana en que los ciberdelincuentes rivales intentaron "doxearlo" (su dox nombró al individuo equivocado, pero incluyó algunas de las identidades más reservadas de Ika).

"No es ningún secreto que el karma se tiró un pedo en mi dirección", dijo Ika al comienzo de su publicación. Sin que Ika lo supiera en ese momento, su foro Pustota también había sido completamente pirateado esa semana y se compartió una copia de su base de datos con este autor.

Una versión traducida por Google de la publicación de despedida de Ika, el administrador de Pustota, un foro sobre cibercrimen en ruso centrado en botnets y spam. Click para agrandar.

Ika dijo que las dos personas que intentaron engañarlo lo hicieron en un foro en ruso aún más cauteloso: DirectConnection[.]ws, quizás la comunidad rusa de cibercrimen más exclusiva jamás creada. Los nuevos solicitantes de este foro tuvieron que pagar un depósito no reembolsable y recibir vales de tres ciberdelincuentes establecidos que ya estaban en el foro. Incluso si uno lograra robar (o adivinar) la contraseña de DirectConnection de un usuario, no se podría acceder a la página de inicio de sesión a menos que el visitante también poseyera un certificado de navegador especial que el administrador del foro otorgaba sólo a los miembros aprobados.

En términos muy claros, Ika declaró que Rescator tenía el sobrenombre de MikeMike en DirectConnection:

“No quería llevar nada de esto a la vida real. Sobre todo porque conocía al patrón de los payasos, concretamente a Pavel Vrublevsky. Sí, afirmo con seguridad que el hombre apodado Rescator, también conocido como MikeMike, y su socio Pipol son desde hace mucho tiempo marionetas de Pavel Vrublevsky”.

Pavel Vrublevsky es un cibercriminal convicto que se hizo famoso como director ejecutivo de la empresa rusa de pagos electrónicos ChronoPay, especializada en

facilitar pagos en línea para una variedad de negocios de “alto riesgo”, incluidos juegos de azar, archivos MP3 pirateados, software antivirus fraudulento y píldoras de “mejora masculina”.

Como se detalla en mi libro Spam Nation de 2014, Vrublevsky dirigió no tan secretamente un programa de spam afiliado a una farmacia llamado Rx-Promotion, que pagaba a spammers y creadores de virus para que enviaran decenas de miles de millones de correos electrónicos basura anunciando Viagra genérico y productos farmacéuticos controlados como analgésicos. medicamentos. Gran parte de mis informes sobre el imperio del cibercrimen de Vrublevsky provinieron de varios años de correos electrónicos y documentos internos de ChronoPay que se filtraron en línea en 2010 y 2011.

Antigua foto del perfil de Facebook de Pavel Vrublevsky.

Continuar leyendo →

Parche de Microsoft Edición del martes de diciembre de 2023

12 de diciembre de 202310 comentarios

El último martes de parches de 2023 está a la vuelta de la esquina: Microsoft Corp. ha publicado hoy soluciones para un número relativamente pequeño de agujeros de seguridad en sus sistemas operativos Windows y otro software. Aún más inusual, no se conocen amenazas de “día cero” dirigidas a ninguna de las vulnerabilidades del lote de parches de diciembre. Aún así, cuatro de las actualizaciones lanzadas hoy abordan vulnerabilidades "críticas" que, según Microsoft, pueden ser explotadas por malware o descontentos para tomar el control total sobre un dispositivo Windows vulnerable con poca o ninguna ayuda de los usuarios.

Entre los errores críticos anulados este mes se encuentra CVE-2023-35628, una debilidad presente en Windows 10 y versiones posteriores, así como en Microsoft Server 2008 y posteriores. Kevin Breen, director senior de investigación de amenazas en Immersive Labs, dijo que la falla afecta a MSHTML, un componente central de Windows que se utiliza para representar contenido basado en navegador. Breen señala que MSHTML también se puede encontrar en varias aplicaciones de Microsoft, incluidas Office, Outlook, Skype y Teams.

"En el peor de los casos, Microsoft sugiere que simplemente recibir un correo electrónico sería suficiente para activar la vulnerabilidad y permitir que el atacante ejecute el código en la máquina

objetivo sin ninguna interacción del usuario, como abrir o interactuar con el contenido", dijo Breen. Continuar leyendo →

ICANN lanza servicio para ayudar con búsquedas de WHOIS

diciembre 6, 202326 Comentarios

Más de cinco años después de que los registradores de nombres de dominio comenzaran a redactar datos personales de todos los registros de registro de dominio público, la organización sin fines de lucro que supervisa la industria de dominios ha introducido un servicio centralizado en línea diseñado para facilitar que los investigadores, las fuerzas del orden y otros soliciten la información. directamente de los registradores.

En mayo de 2018, la Corporación de Internet para la Asignación de Nombres y Números (ICANN), la entidad sin fines de lucro que administra el sistema global de nombres de dominio, ordenó a todos los registradores que eliminaran el nombre, la dirección, el número de teléfono y el correo electrónico del cliente de WHOIS, el sistema para consultar bases de datos. que almacenan los usuarios registrados de nombres de dominio y bloques de rangos de direcciones de Internet.

ICANN realizó el cambio de política en respuesta al Reglamento General de Protección de Datos (GDPR), una ley promulgada por el Parlamento Europeo que requiere que las empresas obtengan consentimiento afirmativo para cualquier información personal que recopilen sobre personas dentro de la Unión Europea. Mientras tanto, los registradores debían continuar recopilando los datos pero no publicarlos, y la ICANN prometió que desarrollaría un sistema que facilitara el acceso a esta información.

A finales de noviembre de 2023, la ICANN lanzó el Servicio de Solicitud de Datos de Registro (RDRS), que está diseñado como una ventanilla única para enviar solicitudes de datos de registro a los registradores participantes. Este video de ICANN explica cómo funciona el sistema.

Los registradores acreditados no tienen que participar, pero la ICANN les pide a todos los registradores que se unan y dice que los participantes pueden optar por no participar o dejar de usarlo en cualquier momento. ICANN sostiene que el uso de un formulario de solicitud estandarizado facilita que se proporcione la información correcta y los documentos de respaldo para evaluar una solicitud.

ICANN dice que el RDRS no garantiza el acceso a los datos de registro solicitados y que toda la comunicación y divulgación de datos entre los registradores y los solicitantes se realiza fuera del sistema. El servicio no se puede utilizar para solicitar datos de WHOIS vinculados a dominios de nivel superior con código de país (CCTLD), como los que terminan en .de (Alemania) o .nz (Nueva Zelanda), por ejemplo. Continuar leyendo →

Okta: La infracción afectó a todos los usuarios de atención al cliente

noviembre 29, 202325 Comentarios

Cuando KrebsOnSecurity dio la noticia el 20 de octubre de 2023 de que el gigante de la identidad y la autenticación Okta había sufrido una violación en su departamento de atención al cliente, Okta dijo que la intrusión permitió a los piratas informáticos robar datos confidenciales de menos del uno por ciento de sus más de 18.000 clientes. Pero hoy, Okta revisó esa declaración de impacto y dijo que los atacantes también robaron el nombre y la dirección de correo electrónico de casi todos sus usuarios de atención al cliente.

Okta reconoció el mes pasado que durante varias semanas a partir de finales de septiembre de 2023, los intrusos tuvieron acceso a su sistema de gestión de casos de atención al cliente. Ese acceso permitió a los piratas informáticos robar la autenticación.

tokens de algunos clientes de Okta, que los atacantes podrían usar para realizar cambios en las cuentas de los clientes, como agregar o modificar usuarios autorizados.

En sus informes iniciales de incidentes sobre la violación, Okta dijo que los piratas informáticos obtuvieron acceso no autorizado a archivos dentro del sistema de atención al cliente de Okta asociados con 134 clientes de Okta, o menos del 1% de la base de clientes de Okta.

Pero en una declaración actualizada publicada esta mañana temprano, Okta dijo que determinó que los intrusos también robaron los nombres y direcciones de correo electrónico de todos los usuarios del sistema de atención al cliente de Okta.

"Todos los clientes de Okta Workforce Identity Cloud (WIC) y Customer Identity Solution (CIS) se ven afectados, excepto los clientes de nuestros entornos FedRamp High y DoD IL4 (estos entornos utilizan un sistema de soporte independiente al que NO accede el actor de amenazas)", afirma el aviso de Okta. "El sistema de gestión de casos de soporte Auth0/CIC tampoco se vio afectado por este incidente". Continuar leyendo →

Servicio de robo de identidad revendido acceso a datos de USInfoSearch

noviembre 28, 202317 Comentarios

Uno de los vendedores más activos de números de seguridad social, antecedentes e informes crediticios del mundo del cibercrimen ha estado extrayendo datos de cuentas pirateadas en el corredor de datos del consumidor estadounidense USinfoSearch, según se enteró KrebsOnSecurity.

Al menos desde febrero de 2023, un servicio anunciado en Telegram llamado USiSLookups ha operado un robot automatizado que permite a cualquiera buscar el SSN o el informe de antecedentes de prácticamente cualquier estadounidense. Para precios que oscilan entre $ 8 y $ 40 y se pueden pagar mediante moneda virtual, el bot devolverá informes detallados de los antecedentes del consumidor automáticamente en tan solo unos momentos.

USiSLookups es el proyecto de un cibercriminal que utiliza los apodos JackieChan/USInfoSearch, y el canal de Telegram para este servicio presenta una pequeña cantidad de ejemplos de informes de antecedentes, incluido el del presidente Joe Biden y el podcaster Joe Rogan. Los datos en esos informes incluyen la fecha de nacimiento, dirección, direcciones anteriores, números de teléfono y empleadores anteriores del sujeto, familiares y asociados conocidos, e información de la licencia de conducir.

El servicio de JackieChan abusa del nombre y las marcas comerciales del corredor de datos USinfoSearch con sede en Columbus, OH, cuyo sitio web dice que proporciona "información de identidad y antecedentes para ayudar con la gestión de riesgos, la prevención del fraude, la verificación de identidad y edad, el rastreo de omisiones y más".

"Nos especializamos en datos no pertenecientes a la FCRA de numerosas fuentes patentadas para brindarle la información que necesita, cuando la necesita", explica el sitio web de la empresa. "Nuestros servicios incluyen acceso basado en API para quienes integran datos en su producto o aplicación, así como procesamiento masivo y por lotes de registros para adaptarse a cada cliente".

Quiso la suerte que mi informe también apareciera en el canal Telegram de este servicio de fraude de identidad, presumiblemente como un adelanto para los posibles clientes. El 19 de octubre de 2023, KrebsOnSecurity compartió una copia de este archivo con el USinfoSearch real, junto con una solicitud de información sobre la procedencia de los datos.

USinfoSearch dijo que investigaría el informe, que parece haber sido obtenido el 30 de junio de 2023 o antes. El 9 de noviembre de 2023, Scott Hostettler, gerente general de Martin Data LLC, matriz de USinfoSearch, compartió una declaración escrita sobre su investigación que sugería que El servicio de robo de identidad intentaba hacer pasar los datos del consumidor de otra persona como si procedieran de USinfoSearch:

Con respecto al incidente de Telegram, entendemos la importancia de proteger la información confidencial y mantener la confianza de nuestros usuarios es nuestra principal prioridad. Cualquier acusación de que hemos proporcionado datos a delincuentes va en directa oposición a nuestros principios fundamentales y a las medidas de protección que hemos establecido y monitoreamos continuamente para evitar cualquier divulgación no autorizada. Debido a que Martin Data tiene reputación de ofrecer datos de alta calidad, los ladrones pueden robar datos de otras fuentes y luego disfrazarlos como si fueran nuestros. Si bien implementamos medidas de seguridad adecuadas para garantizar que solo aquellos a quienes se les permite legalmente acceder a nuestros datos, partes no autorizadas seguirán intentando acceder a nuestros datos. Afortunadamente, los requisitos necesarios para aprobar nuestro proceso de acreditación son difíciles incluso para empresas honestas establecidas.

La declaración de USinfoSearch no abordó ninguna pregunta formulada a la empresa, como si requiere autenticación multifactor para las cuentas de los clientes o si mi informe en realidad provino de los sistemas de USinfoSearch.

Después de muchas insistencias, el 21 de noviembre Hostettler reconoció que el servicio de fraude de identidad USinfoSearch en Telegram estaba en realidad extrayendo datos de una cuenta que pertenecía a un cliente examinado de USinfoSearch.

"Sé al 100% que mi empresa no dio acceso al grupo que creó los bots, pero sí obtuvo acceso a un cliente", dijo Hostettler sobre el servicio de fraude de identidad basado en Telegram. "Pido disculpas por cualquier inconveniente que esto haya causado".

Hostettler dijo que USinfoSearch examina exhaustivamente a cualquier nuevo cliente potencial y que todos los usuarios deben someterse a una verificación de antecedentes y proporcionar ciertos documentos.

Aun así, dijo, varios estafadores cada mes se presentan como dueños de negocios creíbles o ejecutivos de nivel C durante el proceso de acreditación, completando la solicitud y proporcionando la documentación necesaria para abrir una nueva cuenta.

"El nivel de habilidad y destreza demostrado en la creación de estos documentos de respaldo es increíble", dijo Hostettler. “Las numerosas licencias proporcionadas parecen ser réplicas exactas del documento original. Afortunadamente, he descubierto varios métodos de verificación que no se basan únicamente en esos documentos para atrapar a los estafadores”.

"Estas personas son implacables y actúan sin tener en cuenta las consecuencias", continuó Hostettler. “Después de negarles el acceso, se comunicarán con nosotros nuevamente dentro de una semana usando las mismas credenciales. En el pasado, notifiqué tanto a la persona cuya identidad se utiliza de manera fraudulenta como a la policía local. Ambos dudan en actuar porque no se le puede hacer nada al delincuente si no es detenido. Ahí es donde se necesita más atención”. Continuar leyendo →

Presunto extorsionador de pacientes de psicoterapia se enfrenta a juicio

noviembre 16, 202338 Comentarios

Los fiscales de Finlandia comenzaron esta semana su juicio penal contra Julius Kivimäki, un finlandés de 26 años acusado de extorsionar a una práctica de psicoterapia en línea, alguna vez popular y ahora en quiebra, y a miles de sus pacientes. En un informe de 2.200 páginas, las autoridades finlandesas expusieron cómo relacionaban la ola de extorsión con Kivimäki, un notorio hacker que fue condenado en 2015 por perpetrar decenas de miles de delitos cibernéticos, incluidas violaciones de datos, fraude de pagos, operación de una botnet y llamadas con bombas. amenazas.

En noviembre de 2022, Kivimäki fue acusado de intentar extorsionar al Centro de Psicoterapia Vastaamo. En esa violación, que ocurrió en octubre de 2020, un hacker que usaba el alias “Ransom Man” amenazó con publicar notas de psicoterapia de pacientes si Vastaamo no pagaba una demanda de rescate de seis cifras.

Vastaamo se negó, por lo que Ransom Man pasó a extorsionar a pacientes individuales, enviándoles correos electrónicos específicos amenazándolos con publicar sus notas de terapia a menos que pagaran un rescate de 500 euros. Cuando Ransom Man tuvo poco éxito extorsionando a los pacientes directamente, subieron a la web oscura un gran archivo comprimido que contenía todos los registros de pacientes de Vastaamo robados.

Los expertos en seguridad pronto descubrieron que Ransom Man había incluido por error una copia completa de su carpeta de inicio, donde los investigadores encontraron muchas pistas que

apuntaban a la participación de Kivimäki. En ese momento, Kivimäki ya no estaba en Finlandia, pero el gobierno finlandés acusó a Kivimäki in absentia del hackeo de Vastaamo. El documento de evidencia de 2.200 páginas contra Kivimäki sugiere que disfrutó de un estilo de vida lujoso mientras estaba prófugo, frecuentando complejos turísticos de lujo y alquilando autos y viviendas fabulosamente caras.

Pero en febrero de 2023, Kivimäki fue arrestado en Francia después de que las autoridades respondieran a una llamada de disturbios domésticos y encontraran al acusado durmiendo con resaca en el sofá de una mujer que había conocido la noche anterior. La policía francesa empezó a sospechar cuando el hombre rubio de ojos verdes, de 6' 3", presentó una identificación que indicaba que era de nacionalidad rumana.

Una copia redactada de una identificación que Kivimaki entregó a las autoridades francesas afirmando que era de Rumania.

Los fiscales finlandeses demostraron que la tarjeta de crédito de Kivimäki se había utilizado para pagar el servidor virtual que alojaba las notas robadas de los pacientes de Vastaamo. Es más, la carpeta de inicio incluida en el archivo de datos de pacientes de Vastaamo también permitió a los investigadores examinar otros proyectos de cibercrimen del acusado, incluidos dominios a los que Ransom Man tenía acceso, así como un largo historial de comandos que había ejecutado en el dispositivo virtual alquilado. servidor.

Algunos de esos dominios supuestamente administrados por Kivimäki se crearon para manchar la reputación de diferentes empresas e individuos. Uno de ellos era un sitio web que afirmaba haber sido escrito por una persona que dirigía la infraestructura de TI de un importante banco en Noruega y que discutía la idea de legalizar el abuso sexual infantil.

Otro dominio albergaba un blog falso que mancillaba la reputación de un hombre de Tulsa, Oklahoma, cuyo nombre aparecía adjunto a publicaciones de blog sobre el apoyo al movimiento del “orgullo blanco” y el llamado al perdón del atacante de Oklahoma City, Timothy McVeigh.

Parece que Kivimäki también intentó mancillar el nombre de este periodista. El documento de 2.200 páginas muestra que Kivimäki poseía y operaba el dominio krebsonsecurity[.]org, que albergaba varias herramientas de piratería que Kivimäki supuestamente utilizó, incluidos programas para escanear masivamente Internet en busca de sistemas vulnerables a fallos de

seguridad conocidos, así como scripts para descifrar nombres de usuario y contraseñas del servidor de bases de datos y descargar bases de datos. Continuar leyendo →

Parche de Microsoft Edición del martes de noviembre de 2023

noviembre 14, 202316 Comentarios

Microsoft lanzó hoy actualizaciones para corregir más de cinco docenas de agujeros de seguridad en sus sistemas operativos Windows y software relacionado, incluidas tres vulnerabilidades de "día cero" que

Microsoft advierte que ya están siendo explotados en ataques activos.

Las amenazas de día cero dirigidas a Microsoft este mes incluyen CVE-2023-36025, una debilidad que permite que el contenido malicioso eluda la función de seguridad SmartScreen de Windows. SmartScreen es un componente integrado de Windows que intenta detectar y bloquear sitios web y archivos maliciosos. El aviso de seguridad de Microsoft para esta falla dice que los atacantes podrían explotarla haciendo que un usuario de Windows haga clic en un enlace trampa a un archivo de acceso directo.

Kevin Breen, director senior de investigación de amenazas en Immersive Labs, dijo que los correos electrónicos con archivos adjuntos .url o registros con procesos generados a partir de archivos .url "deberían ser una alta prioridad para los cazadores de amenazas dada la explotación activa de esta vulnerabilidad en la naturaleza". Continuar leyendo →

Todavía es fácil para cualquiera convertirse en usted en Experian

11 de noviembre de 202360 comentarios

En el verano de 2022, KrebsOnSecurity documentó la difícil situación de varios lectores a quienes les secuestraron sus cuentas en Experian, una de las tres grandes agencias de informes crediticios del consumidor, después de que los ladrones de identidad simplemente volvieran a registrar las cuentas usando una dirección de correo electrónico diferente. Dieciséis meses después, Experian claramente no ha abordado esta enorme falta de seguridad. Lo sé porque mi cuenta en Experian fue pirateada recientemente y la única forma de recuperar el acceso fue recreando la cuenta.

Al ingresar mi número de seguro social y mi fecha de nacimiento en Experian, se demostró que mi identidad estaba vinculada a una dirección de correo electrónico que no autoricé.

Recientemente solicité una copia de mi archivo de crédito a Experian a través de anualcreditreport.com, pero, como de costumbre, Experian se negó a proporcionármela, diciendo que no podían verificar mi identidad. Los intentos de iniciar sesión en mi cuenta directamente en Experian.com también fallaron; el sitio dijo que no reconocía mi nombre de usuario y/o contraseña.

Una solicitud para el nombre de usuario de mi cuenta de Experian requería mi número de Seguro Social completo y mi fecha de nacimiento, después de lo cual el sitio web mostraba partes de una dirección de correo electrónico que nunca autoricé y no reconocí (Experian borró la dirección completa).

Inmediatamente sospeché que Experian todavía permitía que cualquiera recreara su cuenta de archivo de crédito usando la misma información personal pero una dirección de correo electrónico diferente, una falla de autenticación importante que se exploró en la historia del año pasado, Experian, tienes algunas explicaciones que hacer. Así que una vez más intenté volver a registrarme como yo mismo en Experian.

La página de inicio decía que necesitaba proporcionar un número de Seguro Social y un número de teléfono móvil, y que pronto recibiría un enlace en el que debía hacer clic para verificarme. El sitio afirma que el número de teléfono que proporcione se utilizará para ayudar a validar su identidad. Pero parece que se puede proporcionar cualquier número de teléfono en los Estados Unidos en esta etapa del proceso, y el sitio web de Experian no se opondrá. De todos modos, los usuarios pueden simplemente omitir este paso seleccionando la opción "Continuar de otra manera".

Luego, Experian le solicita su nombre completo, dirección, fecha de nacimiento, número de Seguro Social, dirección de correo electrónico y contraseña elegida. Después de eso, requieren que usted responda con éxito entre tres y cinco preguntas de seguridad de opción múltiple cuyas respuestas a menudo se basan en registros públicos. Cuando recreé mi cuenta esta semana, solo dos de las cinco preguntas se referían a mi información real, y ambas preguntas se referían a direcciones postales en las que habíamos vivido anteriormente, información que está a solo una búsqueda en Google.

Suponiendo que navegue por las preguntas de opción múltiple, se le pedirá que cree un PIN de 4 dígitos y proporcione una respuesta a una de varias preguntas de desafío preseleccionadas. Después de eso, se crea su nueva cuenta y se le dirige al panel de control de Experian, que le permite ver su archivo de crédito completo y congelarlo o descongelarlo.

En este punto, Experian enviará un mensaje a la antigua dirección de correo electrónico vinculada a la cuenta, indicando que ciertos aspectos del perfil del usuario han cambiado. Pero este mensaje no es una solicitud de verificación: es solo una notificación de Experian de que los datos de usuario de la cuenta han cambiado, y al usuario original no se le ofrece ningún recurso más que hacer clic en un enlace para iniciar sesión en Experian.com.

Si no tiene una cuenta de Experian, es una buena idea crear una. Porque al menos recibirás uno de estos correos electrónicos cuando alguien se apropie de tu archivo de crédito en Experian.

Y, por supuesto, un usuario que reciba uno de estos avisos descubrirá que las credenciales de su cuenta de Experian ya no funcionan. Tampoco se cuestiona su PIN o recuperación de cuenta, porque esos también han sido cambiados. ¡Su única opción en este momento es volver a crear su cuenta en Experian y robársela a los ladrones de identidad!

Por el contrario, si intenta modificar una cuenta existente en cualquiera de las otras dos principales agencias de informes crediticios del consumidor (Equifax o TransUnion), le pedirán que ingrese un código enviado a la dirección de correo electrónico o al número de teléfono registrado antes de que se puedan realizar cambios. hecho.

Al contactarme para hacer comentarios, Experian se negó a compartir la dirección de correo electrónico completa que se agregó sin autorización a mi archivo de crédito.

"Para asegurar

Para la protección de las identidades y la información de los consumidores, hemos implementado un enfoque de seguridad de múltiples capas, que incluye medidas pasivas y activas, y estamos en constante evolución", dijo el portavoz de Experian, Scott Anderson, en un comunicado enviado por correo electrónico. "Esto incluye preguntas y respuestas basadas en conocimientos, y procesos de verificación de propiedad y posesión de dispositivos".

Anderson dijo que todos los consumidores tienen la opción de activar un método de autenticación multifactor que se solicita cada vez que inician sesión en su cuenta. Pero, ¿de qué sirve la autenticación multifactor si alguien puede simplemente recrear su cuenta con un nuevo número de teléfono y dirección de correo electrónico?