Portal de soporte de Juniper Información expuesta del dispositivo del cliente

febrero 9, 20242 Comentarios

Hasta principios de esta semana, el sitio web de soporte para el proveedor de equipos de red Juniper Networks exponía información potencialmente confidencial relacionada con los productos de los clientes, incluidos los dispositivos que compraban los clientes, así como el estado de la garantía, los contratos de servicio y los números de serie de cada producto. Juniper dijo que desde entonces solucionó el problema y que la exposición inadvertida de los datos se debió a una actualización reciente de su portal de soporte.

Juniper Networks, con sede en Sunnyvale, California, fabrica enrutadores y conmutadores de Internet de alta potencia, y sus productos se utilizan en algunas de las organizaciones más grandes del mundo. A principios de esta semana, KrebsOnSecurity escuchó a un lector responsable de administrar varios dispositivos Juniper, quien descubrió que podía usar el portal de soporte al cliente de Juniper para encontrar información sobre dispositivos y contratos de soporte para otros clientes de Juniper.

Logan George es un pasante de 17 años que trabaja para una organización que utiliza productos Juniper. George dijo que encontró la exposición de datos a principios de esta semana por accidente mientras buscaba información de soporte sobre un producto Juniper en particular.

George descubrió que después de iniciar sesión con una cuenta de cliente normal, el sitio web de soporte de Juniper le permitía enumerar información detallada sobre prácticamente cualquier dispositivo Juniper comprado por otros clientes. La búsqueda en Amazon.com en el portal Juniper, por ejemplo, arrojó decenas de miles de registros. Cada registro incluía el modelo y el número de serie del dispositivo, la ubicación aproximada donde está instalado, así como el estado del dispositivo y la información del contrato de soporte asociado.

Información expuesta por el portal de soporte de Juniper. Las columnas que no se muestran incluyen el número de serie, el número de referencia de soporte de software, el producto, la fecha de vencimiento de la garantía y el ID del contrato.

George dijo que la información del contrato de soporte expuesta es potencialmente confidencial porque muestra qué productos Juniper tienen más probabilidades de carecer de actualizaciones de seguridad críticas.

"Si no tienes un contrato de soporte, no recibes actualizaciones, es tan simple como eso", dijo George. “Usando los números de serie, pude ver qué productos no están sujetos a contratos de soporte. Y luego podría limitar dónde se envió cada dispositivo a través de su sistema de seguimiento de número de serie y, potencialmente, ver todo lo que se envió a la misma ubicación. Muchas empresas no actualizan sus conmutadores con mucha frecuencia y saber qué utilizan permite saber qué vectores de ataque son posibles”.

En una declaración escrita, Juniper dijo que la exposición de los datos fue el resultado de una reciente actualización de su portal de soporte.

"Nos enteramos de un problema involuntario que permitía a los usuarios registrados en nuestro sistema acceder a números de serie que no estaban asociados con su cuenta", se lee en el comunicado. “Actuamos con prontitud para resolver este problema y no tenemos motivos para creer en este momento que ningún dato personal o identificable del cliente haya sido expuesto de alguna manera. Nos tomamos estos asuntos en serio y siempre utilizamos estas experiencias para evitar futuros incidentes similares. Estamos trabajando activamente para determinar la causa raíz de este defecto y agradecemos al investigador por informarnos sobre esto”. Continuar leyendo →

Del cibercrimen Saul Goodman al GRU ruso

febrero 7, 20248 Comentarios

En 2021, el exclusivo foro ruso sobre ciberdelincuencia Mazafaka fue pirateado. La base de datos de usuarios filtrada muestra que uno de los fundadores del foro era un abogado que asesoraba a los principales piratas informáticos de Rusia sobre los riesgos legales de su trabajo y qué hacer si los atrapaban. Una revisión de las identidades de los piratas informáticos de este usuario muestra que durante su estancia en los foros se desempeñó como oficial de las fuerzas especiales del GRU, la agencia de inteligencia militar extranjera de la Federación Rusa.

Lanzada en 2001 bajo el lema “Terrorismo en red”, Mazafaka evolucionaría hasta convertirse en una de las comunidades de ciberdelincuencia de habla rusa más vigiladas. La lista de miembros del foro incluía un Quién es Quién de los principales ciberdelincuentes rusos, y contaba con subforos para una amplia gama de especialidades de delitos cibernéticos, incluidos malware, spam, codificación y robo de identidad.

Una representación de la base de datos filtrada de Mazafaka.

En casi cualquier filtración de base de datos, las primeras cuentas que aparecen suelen ser las de los administradores y los primeros miembros principales. Pero la información del usuario de Mazafaka publicada en línea no era un archivo de base de datos per se, y fue claramente editada, redactada y reestructurada por quien la publicó. Como resultado, puede resultar difícil saber qué miembros son los primeros usuarios.

Se sabe que el Mazafaka original fue lanzado por un hacker que usaba el sobrenombre de "Stalker". Sin embargo, el ID de usuario con el número más bajo (no administrador) en la base de datos de Mazafaka pertenece a otra persona que utilizó el identificador “Djamix” y la dirección de correo electrónico djamix@mazafaka[.]ru.

Desde el inicio del foro hasta aproximadamente 2008, Djamix fue uno de sus contribuyentes más activos y elocuentes. Djamix dijo a los miembros del foro que era abogado y que casi todas sus publicaciones incluían análisis legales de varios casos públicos que involucraban a piratas informáticos arrestados y

acusado de delitos cibernéticos en Rusia y en el extranjero.

“Ocultarse con parámetros puramente técnicos no ayudará en un asunto serio”, advirtió Djamix a los miembros de Maza en septiembre de 2007. “Para ESCAPAR de la ley, es necesario CONOCER la ley. Esta es la cosa más importante. Las capacidades técnicas no pueden superar la inteligencia y la astucia”.

El propio Stalker le dio crédito a Djamix por mantener a Mazafaka en línea durante tantos años. En una publicación retrospectiva publicada en Livejournal en 2014 titulada “Mazafaka, desde su concepción hasta el día de hoy”, Stalker dijo que Djamix se había convertido en un miembro central de la comunidad.

"Este tipo está en todas partes", dijo Stalker sobre Djamix. “No hay nada en [Mazafaka] en el que él no participe. Para mí, es un estímulo irritante y gracias a él, Maza todavía está vivo. ¡Nuestra fuerza de reunión!

Djamix dijo a otros habitantes del foro que era un abogado autorizado que podía ser contratado para consultas remotas o en persona, y sus publicaciones en Mazafaka y otros foros rusos muestran que varios piratas informáticos que enfrentan peligros legales probablemente aceptaron esta oferta.

“Tengo derecho a representar sus intereses ante los tribunales”, dijo Djamix en el foro sobre cibercrimen en ruso Verified en enero de 2011. “De forma remota (en forma de apoyo y consultas constantes) o en persona; esto se discute por separado. Así como el costo de mis servicios”. Continuar leyendo →

¿Arrestos por intercambio de SIM de 400 millones de dólares están vinculados a un atraco en FTX?

febrero 1, 202411 comentarios

Tres estadounidenses fueron acusados esta semana de robar más de 400 millones de dólares en un ataque de intercambio de SIM en noviembre de 2022. El gobierno de EE. UU. no nombró a la organización víctima, pero todo indica que el dinero fue robado del ahora desaparecido intercambio de criptomonedas FTX, que acababa de declararse en quiebra ese mismo día.

Un gráfico que ilustra el flujo de más de 400 millones de dólares en criptomonedas robadas de FTX del 11 al 12 de noviembre de 2022. Imagen: Elliptic.co.

Una acusación formal revelada esta semana y reportada por primera vez por Ars Technica alega que Robert Powell, un hombre de Chicago, también conocido como “R”, “R$” y “ElSwapo1”, era el cabecilla de un grupo de intercambio de SIM llamado “Powell SIM Swapping Crew”. " Emily “Em” Hernandez, residente de Colorado, supuestamente ayudó al grupo a obtener acceso a los dispositivos de las víctimas al servicio de ataques de intercambio de SIM entre marzo de 2021 y abril de 2023. Carter Rohn, residente de Indiana, también conocido como “Carti” y “Punslayer”, supuestamente ayudó a comprometer los dispositivos. .

En un ataque de intercambio de SIM, los delincuentes transfieren el número de teléfono del objetivo a un dispositivo que controlan, lo que les permite interceptar cualquier mensaje de texto o llamada telefónica enviada a la víctima, incluidos códigos de acceso de un solo uso para autenticación o enlaces de restablecimiento de contraseña enviados por SMS.

La acusación afirma que los autores de este atraco robaron los 400 millones de dólares en criptomonedas el 11 de noviembre de 2022 después de que intercambiaron la tarjeta SIM de un

cliente de AT&T haciéndose pasar por ellos en una tienda minorista utilizando una identificación falsa. Sin embargo, el documento se refiere a la víctima en este caso únicamente con el nombre “Víctima 1”.

Andy Greenberg de Wired escribió recientemente sobre la carrera nocturna de FTX para detener un robo de criptomonedas de mil millones de dólares que ocurrió la noche del 11 de noviembre:

“El personal de FTX ya había pasado por uno de los peores días en la corta vida de la empresa. Lo que recientemente había sido uno de los principales intercambios de criptomonedas del mundo, valorado en 32 mil millones de dólares sólo 10 meses antes, acababa de declararse en quiebra. Después de una larga lucha, los ejecutivos habían persuadido al director ejecutivo de la empresa, Sam Bankman-Fried, para que entregara las riendas a John Ray III, un nuevo director ejecutivo ahora encargado de guiar a la empresa a través de una maraña de deudas de pesadilla, muchas de las cuales parecían no tener medios para pagar”.

“Parecía que FTX había tocado fondo. Hasta que alguien (un ladrón o ladrones que aún no han sido identificados) eligió ese momento en particular para empeorar las cosas. Ese viernes por la noche, el exhausto personal de FTX comenzó a ver misteriosas salidas de la criptomoneda de la compañía, capturadas públicamente en el sitio web Etherscan que rastrea la cadena de bloques Ethereum, lo que representa el robo de criptomonedas por valor de cientos de millones de dólares en tiempo real.

La acusación dice que los 400 millones de dólares fueron robados durante varias horas entre el 11 y el 12 de noviembre de 2022. Tom Robinson, cofundador de la firma de inteligencia blockchain Elliptic, dijo que los atacantes en el atraco a FTX comenzaron a vaciar las billeteras de FTX en la noche del 1 de noviembre. 11 de noviembre de 2022, hora local, y continuará hasta el 12 de noviembre.

Robinson dijo que Elliptic no tiene conocimiento de ningún otro robo de criptomonedas de esa magnitud que haya ocurrido en esa fecha.

"Calculamos el valor de los criptoactivos robados en 477 millones de dólares", dijo Robinson. “Los administradores de FTX han informado de pérdidas totales debido a “transferencias no autorizadas a terceros” de 413 millones de dólares; la discrepancia probablemente se deba a la posterior incautación y devolución de algunos de los activos robados. De cualquier manera, ciertamente son más de $400 millones, y no tenemos conocimiento de ningún otro robo de intercambios de cifrado a esta escala, en esta fecha”. Continuar leyendo →

Hombre de Florida acusado de intercambio de tarjetas SIM es el principal sospechoso de grupos de hackers