PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

185-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°185	Fecha: 12-08-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Cómo los ataques de phishing se adaptan rápidamente para sacar provecho de los acontecimientos actuales		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

En 2023, no menos del 94% de las empresas se vieron afectadas por ataques de phishing, un aumento del 40 por ciento en comparación con el año anterior, según una investigación de Egress.

En la era digital actual, la Inteligencia Artificial (IA) se ha convertido en una herramienta de doble filo en el mundo de la ciberseguridad. Mientras que la IA se utiliza para fortalecer las defensas cibernéticas, también está transformando la forma en que se propagan los ataques cibernéticos; en particular, la IA generativa, que ha hecho que sea mucho más fácil para los actores de amenazas crear contenido que pueden usar en campañas de phishing, como correos electrónicos maliciosos y videos deepfake. Incluso puede ayudar a escribir el malware que los actores de amenazas suelen colocar en las computadoras y servidores de sus víctimas como parte de las campañas de phishing.

2. DETALLES:

Tradicionalmente, estos ataques se basaban en técnicas de ingeniería social para engañar a las personas y conseguir que divulgaran información confidencial. Sin embargo, con la llegada de la IA, los ciberdelincuentes han adquirido una ventaja alarmante en sus actividades maliciosas.

Gracias a algoritmos de aprendizaje automático y análisis de datos, la IA puede identificar patrones de comportamiento sospechoso, detectar vulnerabilidades y prevenir ataques antes de que ocurran. Sin embargo, los ciberdelincuentes no se quedan atrás y han encontrado formas creativas de utilizar la IA para su beneficio.

Uno de los principales impactos de la IA en la propagación de los ataques cibernéticos es su capacidad para automatizar y personalizar los ataques. Los hackers pueden utilizar algoritmos de IA para adaptar sus métodos a los sistemas y las redes objetivo de manera mucho más eficiente que antes. Esto hace que los ataques sean más sigilosos y difíciles de detectar para las soluciones de seguridad tradicionales.

El phishing como servicio (PhasaaS, por sus siglas en inglés) es otro de los avances que se citan a veces para explicar por qué las amenazas de phishing están en su punto más alto. Al permitir que las partes malintencionadas contraten a atacantes expertos para que lleven a cabo campañas de phishing en su nombre, PhaaS facilita que cualquiera que tenga rencor (o el deseo de exfiltrar algo de dinero de víctimas desprevenidas) lance ataques de phishing.

El phishing tiene la costumbre de aprovecharse de los acontecimientos actuales en el mundo para sacar provecho del entusiasmo o el miedo que los rodea. Esto es especialmente cierto cuando se trata de acontecimientos en evolución, como la "pantalla azul de la muerte" (BSOD) de CrowdStrike.

CrowdStrike solucionó el problema con relativa rapidez, pero no antes de que los actores de amenazas comenzaran a lanzar campañas de phishing diseñadas para aprovecharse de las personas y las empresas que buscaban una solución al problema. En el primer día posterior al incidente de CrowdStrike, Cyberint detectó 17 dominios que se dedicaban a la piratería de errores ortográficos relacionados con el problema. Los dominios fueron dados de baja, pero no antes de que las organizaciones cayeran víctimas de ellos.

Cuando se trata de eventos planificados, los ataques suelen ser más diversos y detallados. Los actores de amenazas tienen más tiempo para prepararse que en el caso de eventos inesperados como la interrupción del servicio de CrowdStrike.

Por ejemplo, en el contexto de los Juegos Olímpicos de 2024 en París, Cyberint detectó correos electrónicos de phishing que afirmaban que los destinatarios habían ganado entradas para los Juegos y que, para recogerlas, necesitaban hacer un pequeño pago para cubrir la tarifa de envío.

Sin embargo, si los destinatarios ingresaban su información financiera para pagar la tarifa, los atacantes la usaban para hacerse pasar por víctimas y realizar compras usando sus cuentas.

En otro ejemplo de phishing vinculado a los Juegos Olímpicos, en marzo de 2024, los actores de amenazas registraron un sitio web de apariencia profesional que afirmaba ofrecer entradas a la venta. En realidad, era un fraude.

Se produjeron ataques similares durante la Eurocopa 2024 de fútbol. En particular, los actores de amenazas lanzaron aplicaciones móviles fraudulentas que se hacían pasar por la UEFA, la asociación deportiva que organizó el evento. Como las aplicaciones usaban el nombre y el logotipo oficiales de la organización, era de suponer que a algunas personas les resultó fácil asumir que eran legítimas.

Cuando se trata de eventos recurrentes, los phishers también saben cómo aprovechar las situaciones para lanzar ataques poderosos.

Por ejemplo, los fraudes con tarjetas de regalo, las estafas por falta de pago y los recibos de pedidos falsos aumentan durante la temporada navideña. Lo mismo ocurre con las estafas de phishing que intentan engañar a las víctimas para que soliciten empleos de temporada falsos con el fin de recopilar su información personal.

Las vacaciones crean una tormenta perfecta para el phishing debido al aumento de las compras en línea, las ofertas atractivas y una avalancha de correos electrónicos promocionales. Los estafadores aprovechan estos factores, lo que genera importantes daños financieros y de reputación para las empresas.

El spear phishing, por ejemplo, una forma muy selectiva de phishing, se ha vuelto cada vez más sofisticado con la integración de la IA. Aprovechando los algoritmos de aprendizaje automático, los atacantes pueden analizar grandes cantidades de datos para elaborar mensajes personalizados y convincentes que eluden las medidas de seguridad tradicionales. A menudo, estos mensajes parecen proceder de fuentes de confianza, como bancos u organizaciones acreditadas, lo que los hace aún más engañosos.

Las técnicas de generación de lenguaje natural (NLG) basadas en IA permiten a los ciberdelincuentes generar contenidos persuasivos y contextualmente relevantes que imitan la comunicación humana. Mediante el uso de NLG, los correos electrónicos y mensajes de phishing se pueden personalizar para explotar vulnerabilidades específicas o sacar provecho de eventos actuales, lo que los hace más propensos a engañar a sus objetivos.

La tecnología Deepfake amplifica aún más el daño potencial causado por los ataques de phishing impulsados por IA. Con las falsificaciones profundas, los atacantes pueden crear contenidos de audio y vídeo realistas que suplantan la identidad de personas u organizaciones.

Por ejemplo, en el ámbito nacional hay avisos sospechosos que ofrecen dinero rápido, utilizando inteligencia artificial. El aviso promueve la inversión de grandes sumas de dinero con la promesa de altas ganancias. Incluso se puede notar claramente la voz doblada que no pertenece al personaje en cuestión. Estarían usando la plataforma llamada Cripto Perú. La oferta esta generado numerosos comentarios de usuarios que indican que podría tratarse de una estafa.

Este tipo de anuncios fraudulentos suele aprovecharse de la reputación de empresas reconocidas, como por ejemplo Google, para ganar la confianza de los usuarios.

Al pedir datos personales para reclamar el premio, los estafadores obtienen información que pueden usar para realizar fraudes financieros, suplantación de identidad, y otras actividades delictivas.

Este tipo de avisos invita a los usuarios a cobrar este supuesto premio llenando sus datos personales. Esta táctica es comúnmente utilizada por estafadores para obtener información sensible que luego puede ser utilizada en fraudes y otros delitos cibernéticos.

3. RECOMENDACIONES:

- Anticipar picos de ataques en respuesta a desarrollos específicos o (en el caso de campañas de phishing recurrentes) épocas del año y tomar medidas para mitigar el riesgo.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Implementar la autenticación multifactor para lograr añadir una capa adicional de seguridad exigiendo a los usuarios varias formas de verificación.
- Tener copias de seguridad de los datos de forma que la recuperación ante un posible ransomware no afecte o lo haga lo menos posible a la continuidad del negocio de la compañía.
- Aprovechar los sistemas avanzados de detección de amenazas que utilizan IA y aprendizaje automático puede ayudar a identificar y bloquear ataques de phishing sofisticados. Estos sistemas pueden analizar patrones, detectar anomalías y responder de forma proactiva a posibles amenazas, proporcionando una mayor protección frente a las técnicas de ataque en evolución.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Educar a los empleados y consumidores para que sean más cautelosos al responder a contenido asociado con un evento actual.

Fuente de Información:	• hxxps://thehackernews.com/2024/08/how-phishing-attacks-adapt-quickly-to.html • hxxps://www.la.logicalis.com/es/Como-afecta-la-IA-en-la-propagacion-de-los-ataques-ciberneticos#:~:text=Los%20ciberdelincuentes%20pueden%20generar%20correos,digitales%20y%20revelen%20informaci%C3%B3n%20confidencial. • hxxps://www.redseguridad.com/entrevistas/la-ia-se-esta-usando-para-generar-ataques-sofisticados-de-phishing_20240503.html • hxxps://www.metacompliance.com/es/blog/phishing-and-ransomware/how-ai-enables-sophisticated-phishing-attacks

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°185	Fecha: 12-08-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de día cero en múltiples versiones en Microsoft Office		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo exposición de información confidencial a un actor no autorizado que afecta a múltiples versiones de Microsoft Office. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la divulgación no autorizada de información confidencial a través de la suplantación de identidad en Microsoft Office.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-38200 de tipo de exposición de información confidencial a un actor no autorizado en Microsoft Office, la explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la divulgación no autorizada de información confidencial.

En un escenario de ataque basado en la web, un atacante podría alojar un sitio web (o aprovechar un sitio web comprometido que acepte o aloje contenido proporcionado por el usuario) que contenga un archivo especialmente diseñado para explotar la vulnerabilidad. Sin embargo, un atacante no tendría forma de obligar al usuario a visitar el sitio web. En su lugar, un atacante tendría que convencer al usuario de hacer clic en un enlace, normalmente mediante un incentivo en un correo electrónico o mensaje de mensajería instantánea, y luego convencer al usuario de abrir el archivo especialmente diseñado.

A. Productos afectados:

- Microsoft Office 2016 (edición de 64 bits).
- Microsoft Office 2016 (edición de 32 bits).
- Microsoft Office LTSC 2021 para ediciones de 32 bits.
- Microsoft Office LTSC 2021 para ediciones de 64 bits.
- Aplicaciones de Microsoft 365 para empresas para sistemas de 64 bits.
- Aplicaciones de Microsoft 365 para empresas para sistemas de 32 bits.
- Microsoft Office 2019 para ediciones de 64 bits.
- Microsoft Office 2019 para ediciones de 32 bits.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°185	Fecha: 12-08-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades de Google ChromeOS		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo lectura fuera de límites, confusión de tipos y usar después de liberar en Google ChromeOS. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto generar una condición de denegación de servicio (DoS) y la ejecución remota de código en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-5497 de tipo lectura fuera de límites, se debe a que el acceso a la memoria fuera de los límites en la interfaz de usuario del navegador en Google Chrome anterior a la versión 125.0.6422.141, podría permitir que un atacante remoto convenciera a un usuario para que realizara gestos específicos de la interfaz de usuario para explotar potencialmente la corrupción del montón a través de una página HTML diseñada.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-6100 de tipo confusión de tipos en la versión 8 de Google Chrome anterior a la 126.0.6478.114, podría permitir a un atacante remoto ejecutar código arbitrario a través de una página HTML creada a medida.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-36971 de tipo usar después de liberar que afecta al kernel de Linux, específicamente al sistema operativo Android, podría permitir que un atacante con privilegios de ejecución del sistema realice una ejecución remota de código en el núcleo. Esta vulnerabilidad se ha caracterizado como un problema de ejecución de código remoto que puede ser explotado por atacantes con privilegios a nivel de sistema. Se ha informado de que se está explotando de forma limitada y dirigida, lo que indica que puede ser utilizada activamente en ciberataques, posiblemente por vendedores de software espía comerciales.

Google ha indicado que la vulnerabilidad CVE-2024-36971 ha sido explotada en ataques dirigidos, aunque no se han revelado detalles específicos sobre estos ataques ni sobre los actores de amenazas implicados.

A. Productos afectados:

- Versión anterior a 120.0.6099.318 (Versión de la plataforma: 15662.115).

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://chromereleases.googleblog.com/2024/07/long-term-support-channel-update-for_25.html • hxxps://source.android.com/docs/security/bulletin/2024-08-01?hl=es-419

Índice alfabético