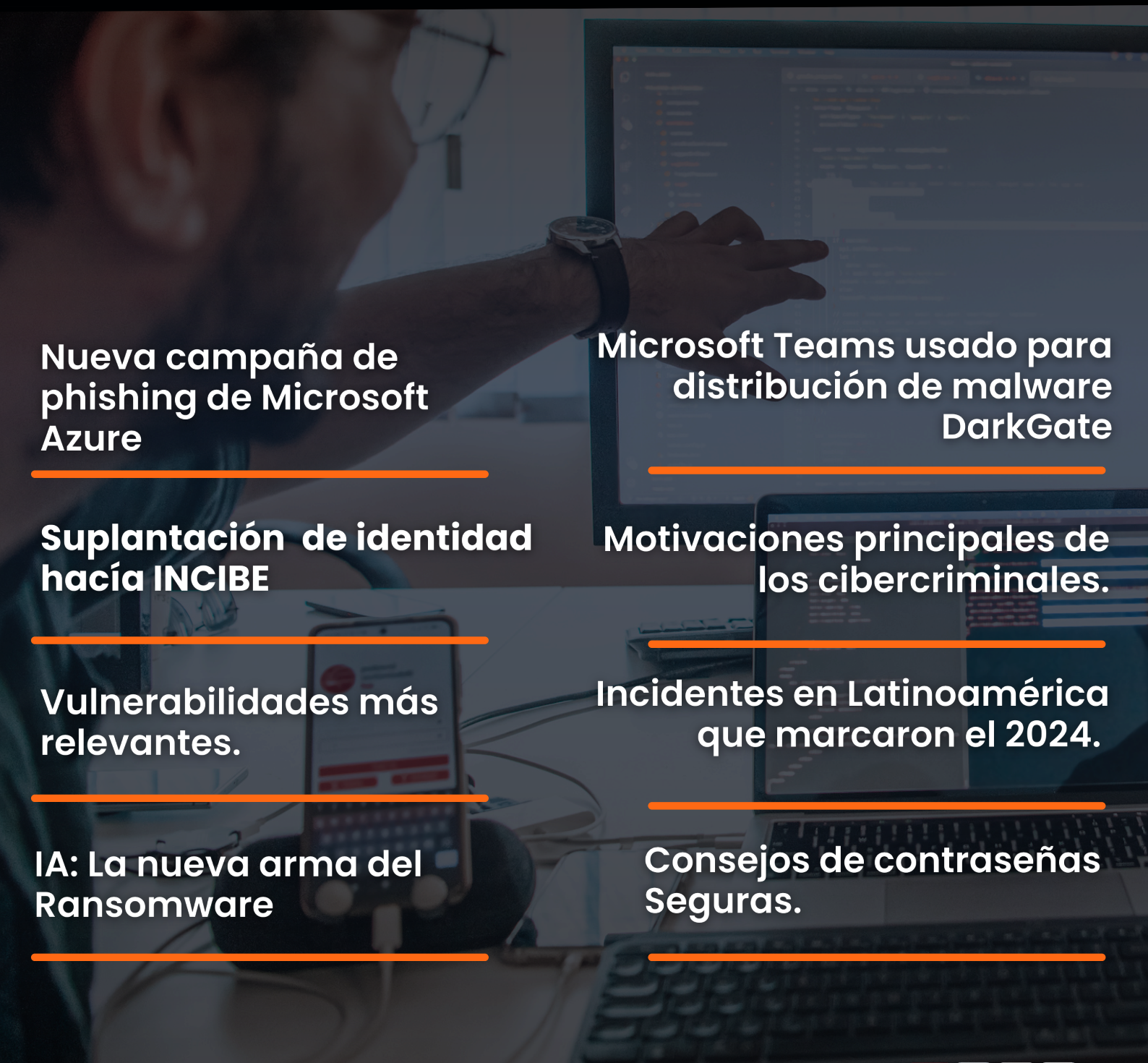
CIBER E-DEA

Boletín de Seguridad



Nueva campaña de phishing de Microsoft Azure

Microsoft Teams usado para distribución de malware DarkGate

Suplantación de identidad hacía INCIBE

Motivaciones principales de los cibercriminales.

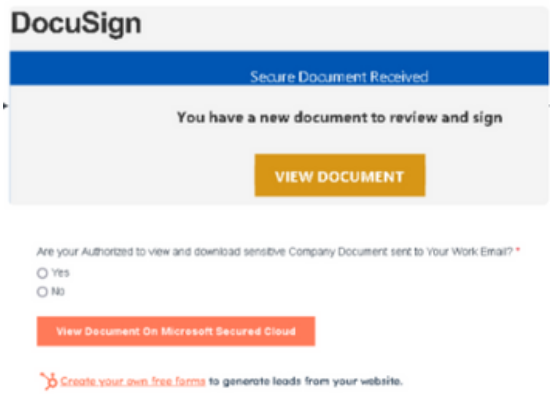
Vulnerabilidades más relevantes.

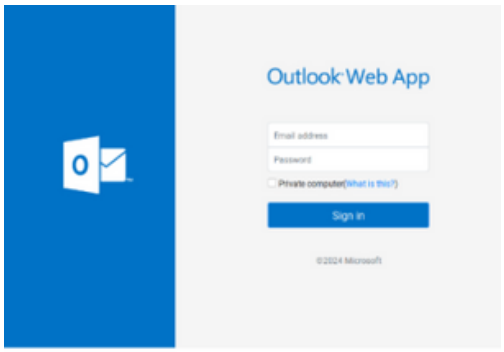
Incidentes en Latinoamérica que marcaron el 2024.

IA: La nueva arma del Ransomware

Consejos de contraseñas Seguras.

Nueva campaña de phishing de Microsoft Azure





Una campaña de phishing compromete 20.000 cuentas de Microsoft Azure donde los atacantes utilizan los formularios en línea de HubSpot como trampa para capturar información confidencial. Donde elaboraron 17 formularios diferentes, diseñados para imitar solicitudes legítimas de Microsoft Azure .

Este mensaje pretendía facilitar el acceso a documentos críticos almacenados en la Nube segura de Microsoft.

Estos formularios preguntaban a las víctimas en un inglés mal redactado si estaban autorizados para ver y descargar un documento confidencial de la empresa enviado a su correo electrónico del trabajo.

Las personas que hacen clic en los formularios eran redirigidas a páginas que se hacían pasar por los portales de inicio de sesión de Microsoft Outlook Web App y Azure, alojados en dominios '.buzz'. Estas tácticas permitieron a los atacantes eludir las medidas de seguridad de correo electrónico estándar, ya que los correos electrónicos de phishing estaban vinculados a un servicio legítimo (HubSpot).

Una vez que los atacantes obtuvieran acceso a las cuentas comprometidas, registraban sus propios dispositivos en las cuentas de las víctimas, asegurando así el acceso continuo.
Los investigadores de Paloalto indicaron que los actores de amenazas se conectaban con frecuencia a través de VPN ubicadas en los mismos países que sus objetivos, lo que les ayudaba a mezclarse.

Más información

Microsoft Teams usado para distribución de malware DarkGate

Los atacantes utilizan Microsoft Teams para distribuir el malware DarkGate mediante tácticas avanzadas de ingeniería social.

Según investigadores de Trend Micro, los ciberatacantes utilizaron Microsoft Teams para simular ser un cliente de confianza y persuadir a la víctima de descargar software de acceso remoto.

El ataque, siguió el enfoque múltiples etapas como:

- Bombardeo de correos electrónicos donde saturaron la bandeja de entrada de las víctimas con miles de correos electrónicos.
- Contacto a través de Microsoft Teams haciéndose pasar por empleados de un proveedor externo para ganar la confianza de la víctima.
- Con el acceso remoto en Anydesk, los atacantes entregaron varias cargas maliciosas, incluyendo el malware DarkGate y un ladrón de credenciales.

Características del Malware DarkGate

- Robo de credenciales.
- Registro de pulsaciones de teclas.
- Captura de pantalla.
- Grabación de audio.
- Control remoto del escritorio

Recomendaciones:

- Habilitar autenticación multifactor (MFA).
- Limitar el uso de herramientas de acceso remoto.
- Bloquear la instalación de aplicaciones no verificadas.
- Concienciar a los empleados sobre tácticas de phishing y vishing.

Más Información

Suplantación de identidad hacia INCIBE

Recientemente, se ha detectado una campaña de suplantación de identidad dirigida al INCIBE donde los atacantes se hacen pasar por representantes de INCIBE para engañar a las víctimas y obtener información confidencial o instalar malware en sus dispositivos.

INCIBE es el Instituto Nacional de Ciberseguridad de españa quien también opera un centro de respuesta a incidentes de seguridad (CSIRT).

En la campaña de phishing se informa falsamente a los usuarios sobre investigaciones en curso relacionadas con contenido para adultos.

Método de ataque:

- Correos electrónicos masivos: Los atacantes envían correos electrónicos en nombre de INCIBE.
- PDF adjunto: Incluyen un documento PDF con detalles falsos sobre la investigación.
- Solicitud de datos personales: Instan a las víctimas a responder rápidamente con documentación personal.

Recomendaciones

- Reportar el correo: Si recibes un correo sospechoso, reportarlo como SPAM
- No entregar información y datos confidenciales.
- Verificar autenticidad y remitente
- Aplicar el Doble factor de autenticación a las cuentas.

Más información

Motivaciones principales de los cibercriminales

Dependiendo del objetivo del cibercriminal, de su modus operandi y de las herramientas que utilice, estas son las principales causas o motivos del ciberataque:

- Beneficio Económico: Obtener dinero mediante fraudes y robos de identidad.
- Robo de Información: Acceder a datos sensibles
- Espionaje: Obtener información confidencial
- Sabotaje: Dañar sistemas, redes y datos.
- Reconocimiento y Logros: En busca de fama por sus habilidades
- Diversión: Hackear por entretenimiento, desafío personal o para demostrar habilidades técnicas.
- Ideología: Motivos políticos, religiosos o sociales.
- Venganza: Atacar a individuos o organizaciones por rencores personales o profesionales.
- Acceso a Recursos: Obtener acceso a recursos tecnológicos, como servidores y redes, para utilizarlos en otros ataques o actividades ilícitas

Los usuarios: el eslabón más débil y la principal vulnerabilidad

La ciberseguridad es una responsabilidad compartida, y los usuarios juegan un papel crucial en la prevención de ciberataques exponemos algunos datos e indicadores que destacan la importancia de la participación activa de los usuarios en la protección de la información:

- 39% de las filtraciones de información se deben a la pérdida de dispositivos móviles en el área de trabajo.
- 1 de cada 3 personas abre correos electrónicos de phishing.
- 4 de cada 5 ciberataques se producen por el uso de contraseñas débiles o robadas.
- El coste medio de una filtración de datos es de 3,6 millones de dólares.

Consejos de contraseñas seguras

Una contraseña segura es la principal defensa contra los ciberdelitos.

Las contraseñas comprometidas les proporcionan a los ciberdelincuentes una oportunidad para acceder a tus cuentas.

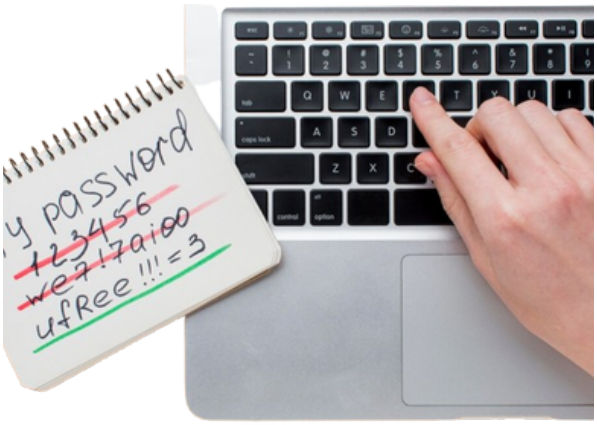
Hoy en día, los ciberdelincuentes usan tecnología sofisticada para obtener tus contraseñas.

¿Qué es una contraseña segura?

Una contraseña segura es una palabra o frase caracterizada por su dificultad de adivinar o descifrar que contiene números, mayúsculas, caracteres especiales.

Errores más comunes en las contraseñas:

- Usar información personal como nombres de familiares o mascotas.
- Utilizar combinaciones fáciles de recordar como “1234” o “password”.
- Utilizar las mismas contraseñas para varias cuentas.
- No cambiar las contraseñas.
- Almacenarlas en una hoja cerca al computador o en el navegador.



Recomendaciones:

- Utiliza una contraseña de mínimo 12 caracteres.
- Utiliza frases que sean fáciles de recordar, ejemplo: ***“Me gusta el color rojo”***
- Usar una combinación de caracteres a la frase:: ***“M3Gust4elC0l0rRojo*”***
- Evitar utilizar información personal.
- Cambia tus contraseñas periódicamente.
- Habilitar el doble factor de autenticación.
- Utiliza un gestor de contraseñas.

Inteligencia Artificial: La nueva arma del Ransomware.

El ransomware ha evolucionado de manera sorprendente, con la inteligencia artificial (IA) desempeñando un papel central. Este cambio ha permitido a los cibercriminales implementar tácticas más sofisticadas, aumentando tanto la efectividad como el alcance de sus ataques.

Un análisis reciente realizado por el Centro de Investigación Avanzada de Trellix revela cómo los grupos de ransomware han adoptado herramientas avanzadas impulsadas por IA para transformar el cibercrimen

La integración de IA en las herramientas de cibercrimen ha revolucionado la manera en que operan los actores maliciosos. Desde la propagación automatizada de malware hasta la personalización de demandas de rescate, estas tecnologías permiten que los cibercriminales se mantengan un paso adelante de las soluciones de seguridad tradicionales.

Un ejemplo destacado es el grupo RansomHub, que se ha convertido en el más activo del mundo, representando el 13 % de las detecciones de Trellix. Este grupo utiliza herramientas como EDRKillShifter, diseñada específicamente para evadir las soluciones de detección y respuesta de puntos finales (EDR), desactivando sus capacidades antes de ejecutar un ataque.

El Futuro del Ransomware y la IA:

El ransomware impulsado por IA no muestra signos de disminuir. Al contrario, la constante evolución de las herramientas y tácticas utilizadas sugiere que esta amenaza continuará creciendo. Para contrarrestar esta tendencia, las organizaciones deben invertir en tecnologías avanzadas de detección, colaborar con las fuerzas del orden y educar a los usuarios sobre los riesgos del cibercrimen.

La combinación de ransomware y inteligencia artificial representa un desafío sin precedentes para la ciberseguridad. Con sectores críticos en riesgo y herramientas avanzadas proliferando en el mercado negro.

Vulnerabilidades destacadas

CVE-2024-49117

Microsoft ha corregido 72 vulnerabilidades en sus productos, dos de las cuales están siendo explotadas activamente.
Una de ellas es CVE-2024-49117, es especialmente alarmante ya que permite a los atacantes ejecución remota de código de Windows Hyper-V

Microsoft - Windows

Versiones afectadas
Todas las versiones.

CVE-2014-7280

TENABLE

Versiones afectadas
Nessus 5.x

Una vulnerabilidad de secuencias de comandos entre sitios (XSS) en la interfaz de usuario de Tenable Nessus 5.x permite que servidores web remotos inyecten secuencias de comandos web o HTML arbitrarios a través del encabezado del servidor.

CVE-2024-3393

Paloalto

Versiones afectadas
PAN-OS

Se identificó una vulnerabilidad en Palo Alto PAN-OS.
Un atacante remoto puede aprovechar esta vulnerabilidad para activar una condición de denegación de servicio en el sistema objetivo.

Incidentes en Latinoamérica que marcaron el 2024.

Banco do Brasil:
En marzo, un ataque permitió a los ciberdelincuentes acceder a las bases de datos del banco, robando datos personales y financieros de más de 2 millones de clientes.

Gobierno de México:
Un ataque de ransomware afectó a varias agencias gubernamentales, paralizando servicios críticos y exponiendo datos sensibles.

Banco de Bogotá (Colombia):
En abril, un ataque de ransomware afectó a los sistemas del banco, paralizando operaciones y exponiendo datos sensibles de clientes.

Air-e (Colombia):
Un ataque de ransomware comprometió los sistemas de la empresa, poniendo en riesgo la continuidad operativa.

Universidad de Buenos Aires (Argentina):
Un ataque dirigido comprometió los sistemas de la universidad, resultando en la pérdida de datos académicos y personales de estudiantes y profesores.

Coppel (Mexico)
En abril sucedió un ciberataque que tuvo como víctima a la cadena mexicana de tiendas Coppel y que afectó a 1.800 tiendas en todo el país

Interbank (Perú):
En octubre, un actor malicioso accedió a datos sensibles de más de 3 millones de clientes utilizando credenciales internas.

Incidentes de seguridad en el mundo.

Filtración de datos de HealthEquity (U.S.A)

En marzo un ataque comprometió la información médica de 4,3 millones de personas, destacando la vulnerabilidad de los datos de salud

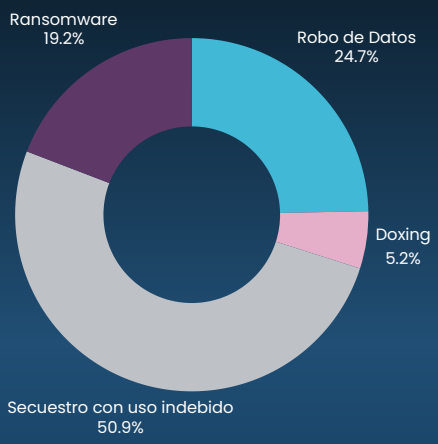
Filtración de Datos en la Fórmula 1 tras Ataques de Phishing

En junio la Federación Internacional del Automóvil (FIA) sufrió un ataque de phishing que comprometió varias cuentas de correo electrónico, exponiendo datos personales.

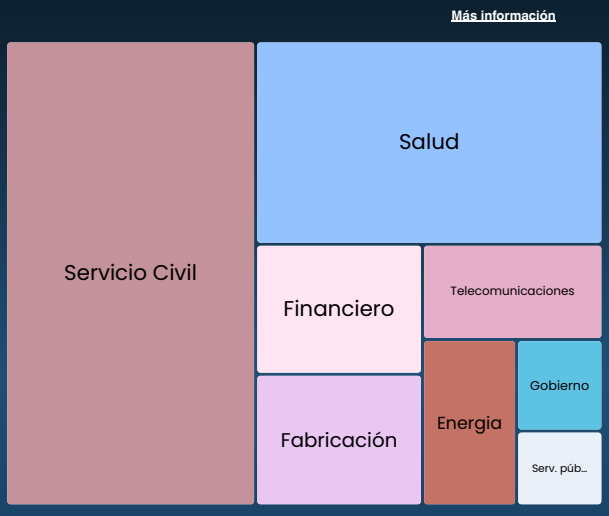
700

Ciber incidentes en 2024

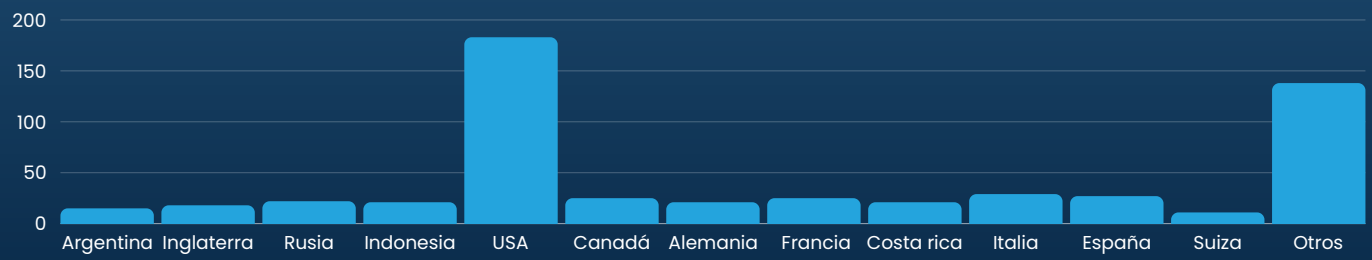
TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS



CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

www.e-dea.co