CIBER E-DEA

Boletín de Seguridad

Mamba 2FA: Nueva amenaza de Phishing

(PhaaS) que se especializa en atacar cuentas de Microsoft 365.

Pérdida de registros en Microsoft

Pérdida de registros críticos de seguridad durante un periodo de casi un mes.

INTERNET ARCHIVE

Víctima de filtración de datos.

ROBOCALLING

Nueva técnica de estafas telefónicas.

Ransomware “Black Basta”

A través de Microsoft Teams.

TIPS

Consejos rápidos a la hora de usar redes WiFi públicas

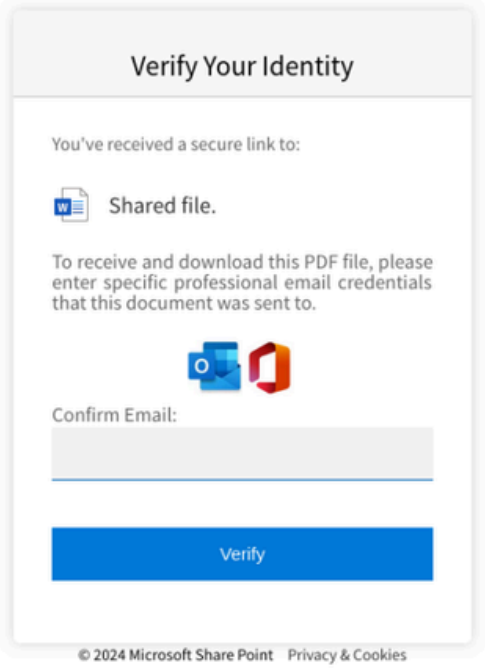
Ciber Incidentes

Incidentes en octubre en Colombia y en el mundo.

e-dea NETWORKS | CYBER SECURITY

Great Place To Work. Certificada NOV 2024 - NOV 2025 CO. icontec ISO 9001 CO-SC-CER890596 icontec ISO 45001 CO-ST-CER890599 icontec ISO / IEC 27001 CO-SI-2001607 IQNET CERTIFIED MANAGEMENT SYSTEM

Mamba 2FA: Nueva amenaza de Phishing



Mamba 2FA es una plataforma de phishing como servicio (PhaaS) que se especializa en atacar cuentas de Microsoft 365.

Similar a otras plataformas PhaaS, emplea relés proxy para llevar a cabo ataques de phishing AiTM, permitiendo a los actores maliciosos acceder a códigos de acceso de un solo uso y cookies de autenticación.

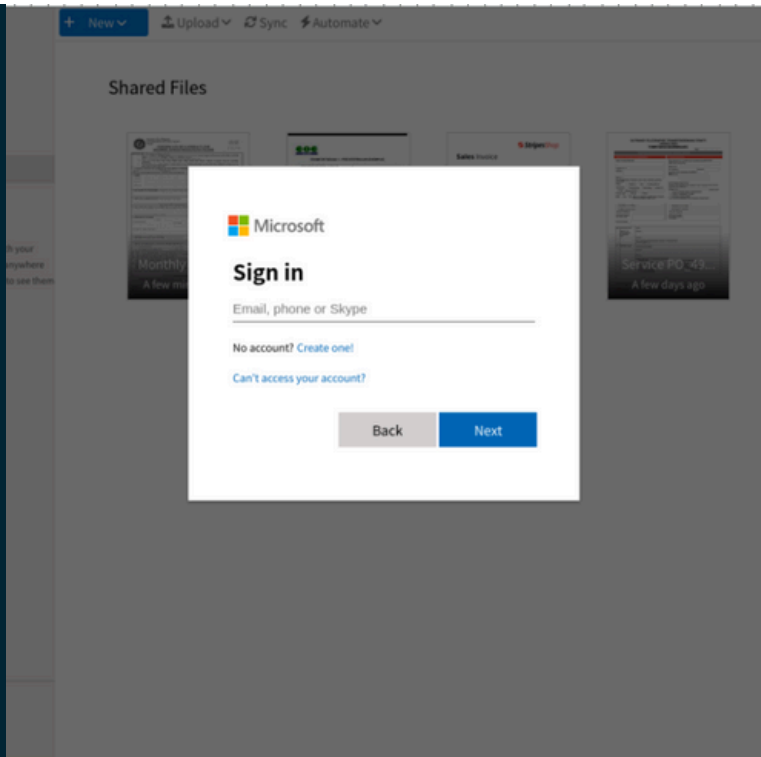
El mecanismo AiTM utiliza la biblioteca JavaScript Socket.IO para establecer comunicación entre la página de phishing y los servidores de retransmisión en el backend, los cuales a su vez se comunican con los servidores de Microsoft utilizando los datos robados.

Las credenciales capturadas y las cookies de autenticación se envían al atacante a través de un bot de Telegram, permitiéndole iniciar sesión de inmediato.

Ofrece una variedad de plantillas de phishing que imitan diferentes servicios de Microsoft 365, como OneDrive, SharePoint Online, páginas de inicio de sesión de Microsoft e incluso falsas notificaciones de correo de voz.

Recomendaciones:

Para protegerse contra las operaciones de PhaaS que utilizan tácticas AiTM, considere usar claves de seguridad de hardware, autenticación basada en certificados, bloqueo geográfico, listas de direcciones IP permitidas, listas de dispositivos permitidos y reducción de la vida útil de los tokens.



Más información

Pérdida de registros en Microsoft

Más Información

Microsoft ha alertado a sus clientes empresariales sobre la pérdida parcial de registros críticos de seguridad durante un periodo de casi un mes, lo que podría comprometer la detección de actividades no autorizadas.

El problema, reportado inicialmente por Business Insider, afectó la recopilación de datos entre el 2 y el 19 de septiembre, extendiéndose hasta el 3 de octubre.

Estos registros son utilizados para monitorear el tráfico, el comportamiento e intentos de inicio de sesión sospechosos.

Según una revisión preliminar de Microsoft, varios servicios fueron afectados:

Azure Logic Apps, Azure Healthcare APIs, Microsoft Sentinel, Azure Monitor y Azure Virtual Desktop.

La compañía explicó que el error se introdujo mientras se solucionaba otro problema en el servicio de recopilación de registros. Aunque el incidente ha sido corregido, el experto en ciberseguridad Kevin Beaumont reporta que al menos dos empresas afectadas no recibieron aviso.

INTERNET ARCHIVE Víctima de filtración de datos

Este sitio web, que almacena una gran parte de la historia del internet, fue hackeado y afectó a más de 31 millones de personas, de las cuales expuso información personal, como direcciones de correo electrónico, nombres de usuario y contraseñas cifradas, entre otros datos de los usuarios.

Más Información

Robocalling: Nueva técnica de estafas telefónicas.

Lo que podría parecer una llamada equivocada o inofensiva, puede ser el primer paso en una estafa. Esta vez, se suma una nueva modalidad de estafa llamada “Robocalling”
Esta es una modalidad donde delincuentes llaman a las víctimas, no responden y finalizan la llamada. Esto les permite verificar que el número está activo para luego incorporarlo en una base de datos para futuras campañas de fraude.

Esta técnica era utilizada habitualmente en campañas de marketing para reproducir mensajes pregrabados a un gran número de destinatarios.

Los delincuentes utilizan esos mismos sistemas automáticos para llamar a múltiples números y así proceder a hacerse pasar por empresas legítimas, enviando mensaje de texto o mensaje por whatsapp y telegram afirmando que la víctima ganó un premio o tiene una compra pendiente.

¿Cómo evitar el robocalling?

- No responder a llamadas sospechosas de números desconocidos o indicativos de otros países.
- Realizar la configuración Anti spam de tu teléfono. Consulta la configuración aquí: Android, Apple
- No proporcionar información personal a fuentes no confiables.
- Acceder a la página de Comisión de Regulación de Comunicaciones (CRC) y registra tu número y correo en el registro de exclusión trámites CRC
- En caso de contestar la llamada cuelga inmediatamente.
- Active el doble factor de autenticación en aplicaciones de mensajería instantánea como whatsapp y telegram.
- Cambie constantemente sus contraseñas.
- Minimice la exposición de su número de teléfono, compartelo solo con personas de confianza.

Más información

Ransomware “Black basta” ataca a través de Microsoft Teams

El grupo de ransomware Black Basta ha adoptado nuevas tácticas para infiltrarse en redes corporativas, esta vez utilizando Microsoft Teams para suplantar al soporte de TI.

Los atacantes comienzan enviando miles de correos electrónicos a los empleados, saturando sus bandejas de entrada con boletines, confirmaciones de registro y verificaciones de correo.

Una vez que el empleado está abrumado por el spam, los atacantes contactan a la víctima a través de Teams, haciéndose pasar por el soporte técnico de microsoft. Durante la conversación, convencen a la víctima de instalar herramientas de acceso remoto como AnyDesk o proporcionar acceso directo a su computadora usando Windows Quick Assist.

Una vez dentro del sistema, los atacantes instalan varias herramientas para mantener el acceso remoto, como ScreenConnect, NetSupport Manager y Cobalt Strike. Con estas herramientas, pueden moverse lateralmente por la red, elevar privilegios, robar datos y finalmente desplegar el ransomware.

Más información

Recomendaciones:

- Limitar las comunicaciones con usuarios externos en Microsoft Teams.
- Habilitar el MFA.

Consejos rápidos a la hora de usar redes WiFi públicas

La conexión a internet se ha vuelto una necesidad constante en nuestra vida. A medida que buscamos acceso a la red en cualquier lugar, las redes wifi públicas se han convertido en una opción.

Sin embargo, al conectarnos a estas redes, existe el riesgo de exponernos a diferentes amenazas de seguridad, entre ellas:

- Interceptación de datos
- Suplantación de identidad
- Malware
- Ataques de phishing
- Ataques Man-in-the-middle (MITM)

Al no contar con una conexión cifrada, cualquier persona en la misma red puede potencialmente acceder a la información que transmitimos como: contraseñas, correos electrónicos y otra información sensible.

Aquí tienes algunos consejos y recomendaciones para mantenerte seguros al conectarte a una red wifi pública:

- Usa contraseñas fuertes y autenticación biométrica.
- Usar una VPN.
- Evita conectarte a redes no seguras.
- No ingresar información personal o sensible.
- Desactiva Bluetooth y ubicación cuando no los uses.
- Realiza copias de seguridad regularmente.
- Cierra sesión en servicios y cuentas al terminar de usar la red.
- Verificar el nombre de la red y su seguridad.
- Revisa los permisos de las aplicaciones.

Vulnerabilidades destacadas

CVE-2024-20498, CVE-2024-20499, CVE-2024-20500, CVE-2024-20501, CVE-2024-2050 Y CVE-2024-20513

Cisco ha revelado recientemente múltiples vulnerabilidades en el servidor VPN Cisco AnyConnect de los dispositivos Cisco Meraki MX y Cisco Meraki Z Series Teleworker Gateway que podrían permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS) al servicio VPN AnyConnect en un dispositivo afectado.

Cisco

Versiones afectadas

Cisco Meraki, VPN Anyconnect

Más información

Microsoft - Windows

Diferentes productos de Microsoft Listado

Más información

CVE-2024-38124 Y CVE-2024-43468

Microsoft publica su listado de actualización de seguridad del mes de octubre, donde se consta de 117 vulnerabilidades donde se califican como críticas, importantes y moderadas.

Ciber incidentes en Colombia y en el mundo

Colombia registra 20.000 millones de ciberataques en lo que va del 2024

El ministro de las TICS Mauricio Lizcano mediante la convención bancaria realizada en Cartagena, indica que en lo que va del año se han registrado veinte mil millones de ciberataques donde el sector financiero es el más afectado.

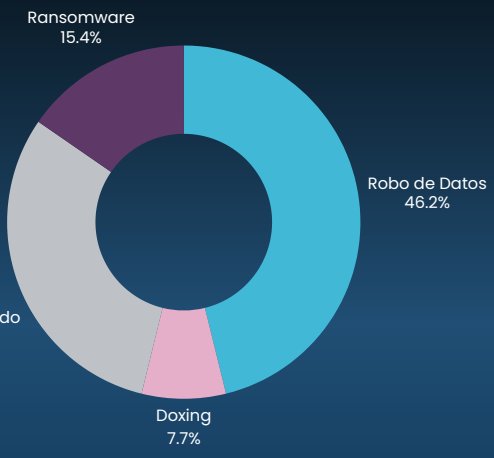
Más información

El mundo

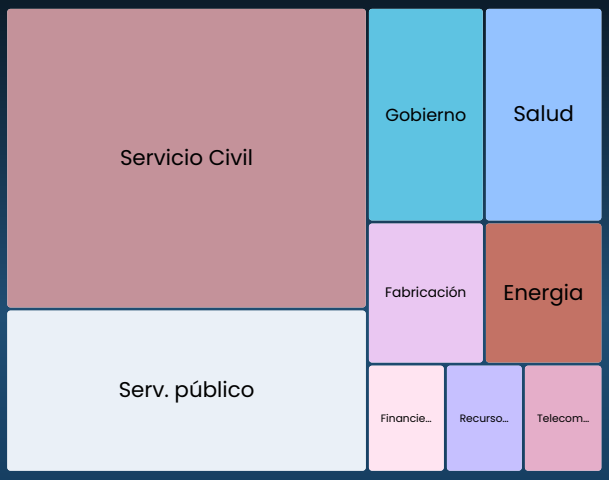
26

Ciber incidentes

TIPO DE INCIDENTE

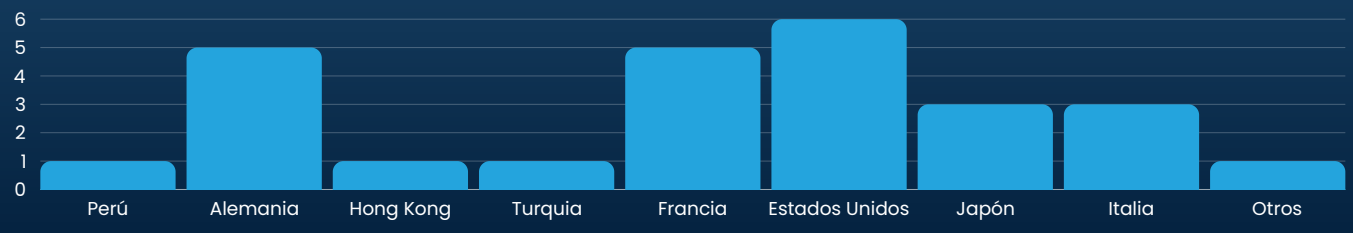


SECTORES AFECTADOS



Más información

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