Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 18/2023**

Cyber noticias

Rapture, la nueva y discreta familia de ransomware. La compañía de ciberseguridad Trend Micro, ha encontrado una nueva cepa de ransomware, el cual se ha dirigido a sus víctimas mediante un enfoque minimalista. La realización de un volcado de memoria durante su ejecución, muestra un archivo de configuración de clave RSA (sistema criptográfico de clave pública), obteniendo una gran similitud con el ransomware Paradise, aunque con un comportamiento diferente. **Fuente:** Escudodigital

Apps fraudulentas que se hacen pasar por ChatGPT. Cada vez hay más apps fraudulentas que se hacen pasar por ChatGPT o por un producto de OpenAI. Es importante recordar que ChatGPT sólo está disponible en la web de OpenAI y no tiene aplicaciones para descargar. ChatGPT solo funciona a través de su plataforma oficial. **Fuente:** Ciberseguridadpyme.

Meta eliminó campaña de malware que usaba ChatGPT como señuelo para captar cuentas. Meta tomó medidas para eliminar más de 1,000 URL's maliciosas que se compartían en sus servicios y descubrió que aprovechaban ChatGPT de OpenAI como un señuelo para propagar malware, utilizando extensiones falsas del navegador web que captaba credenciales de las cuentas de Facebook de los usuarios con el objetivo de ejecutar anuncios no autorizados. **Fuente:** Thehackernews.

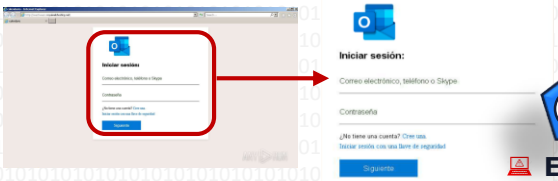
El nuevo malware Fleckpe para Android se instaló 600.000 veces en Google Play. Kaspersky identificó en la Play Store un total de 11 aplicaciones maliciosas, las cuales se hacían pasar por utilidades de edición de fotos y paquetes de fondos de pantalla para teléfonos inteligentes. Cuando se inicia la aplicación, el malware **Fleckpe** carga una biblioteca que contiene un **'dropper'** o **'cuentagotas'** tipo troyano que se descarga en el equipo de la víctima para instalar el malware, con el fin de establecer una conexión con el servidor de comando y control y obtener información del dispositivo infectado. **Fuente:** Securityweek.

Modalidad más reportada al CAI Virtual ¡Phishing!

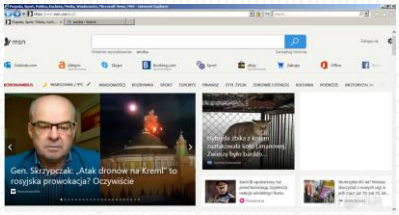
A través del servicio de CAI Virtual, se identificó una campaña de phishing vía correo electrónico, que notifica una falsa suspensión de cuenta email, por actividades no acordes a los servicios y políticas de uso de Microsoft. El objetivo de esta modalidad es realizar la captura de credenciales de acceso y tomar control del mismo.
Este correo está asociado al asunto: **"Hemos detectado alguna actividad que infringe nuestro Contrato de servicios Microsoft".**

1. El correo notifica una presunta suspensión de cuenta correo electrónico por infringir las políticas en los servicios.

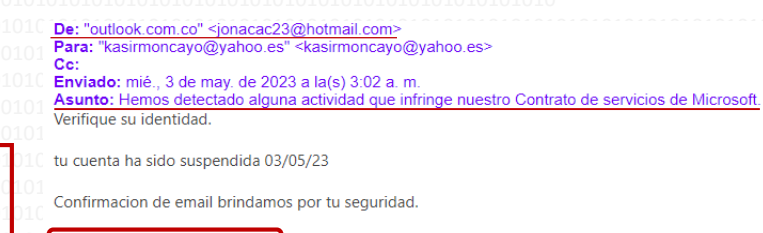
2. Solicita acceder al enlace: **"reactiveacc.royalwebhosting.net"**, que redirecciona a un sitio web falso para validar el inicio de sesión de correo electrónico.



3. Al ingresar los datos para la validar el falso inicio de sesión, se realiza la captura de credenciales de acceso.



Posteriormente, es redireccionado a un sitio web simulando ser la página oficial del correo.



4.

RECOMENDACIONES

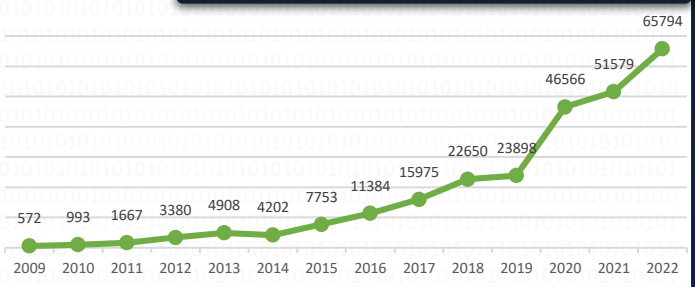
- **EVITE** dar clic sobre links o abrir archivos adjuntos en correos electrónicos desconocidos.
- **VERIFIQUE** ortografía y redacción (usualmente hay errores).
- **VERIFIQUE** que el remitente del correo electrónico, corresponda a una organización legítima.
- **No** ingrese ningún tipo de información en el formulario.
- **UTILICE** la autenticación de dos factores en su cuenta de correo electrónico para aumentar la seguridad y evitar accesos no autorizados.
- **VERIFIQUE** los enlaces o archivos antes de ejecutarlos en un entorno de prueba sandbox (**Ej:** Any.Run, Csirt.Ponal).
- **REPORTE** el correo electrónico allegado a través de nuestro canal de atención del CAI Virtual https://caivirtual.policia.gov.co.

Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2022	2023	
0,73 %	8.333	8.394	Hurto por medios informáticos y semejantes
-8,7 %	4.485	4.185	Violación de datos personales
-4,6 %	4.244	4.046	Acceso abusivo a un sistema informático
-5 %	1.844	1.752	Suplantación de sitios web
-11 %	1.277	1.140	Transferencia no consentida de activos
0,5 %	624	627	Interceptación de datos informáticos
-2,5 %	200	195	Daño informático
57 %	98	154	Uso de software malicioso
-7 %	153	142	Obstaculización ilegítima de sistema informático o red de telecomunicación
TOTAL	**- 3,3 %**	21.359	20.635

Corte del 01 de enero al 05 de mayo2022.
vs 01 de enero al 05 de mayo 2023.

Evolución histórica *(No. Denuncias vs año)*



Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)

Fuente: SIEDCO Plus 2.0

- Bogotá: 31% — 6.431
- Medellín: 8% — 1.654
- Cundinamarca: 7,46% — 1.540
- Cali: 5% — 1.069
- Barranquilla: 4% — 859
- Ibagué: 2% — 417
- Cartagena: 1,81% — 374
- Bucaramanga: 1,67% — 344
- Villavicencio: 1,59% — 328
- Cúcuta: 1,51% — 312

Las denuncias a la fecha representan el **31 %** del total del 2022.
Corte del 01 de enero al 05 de mayo 2023.

Actividades de gestión en seguridad digital

Capturas
Delitos informáticos. 91
Explotación sexual infantil en Internet. 27
118

210
Alertas y contenidos preventivos
08 durante la semana

Incidentes gestionados
a través del CAI Virtual
5.278

68
Actividades de relacionamiento estratégico, resaltando en la semana:
GRUPO ecopetrol ASOBANCARIA

Charlas de ciberseguridad
Personas impactadas **6.011**
49

9.752
Páginas bloqueadas
Material de abuso sexual infantil. 9.196
Juegos ilegales de azar. 556

Para sugerencias sobre este producto, por favor diligencie este formulario :https://bit.ly/3mz5C8d

Canales de atención y redes sociales

Página web | Twitter | Instagram | Facebook | WhatsApp