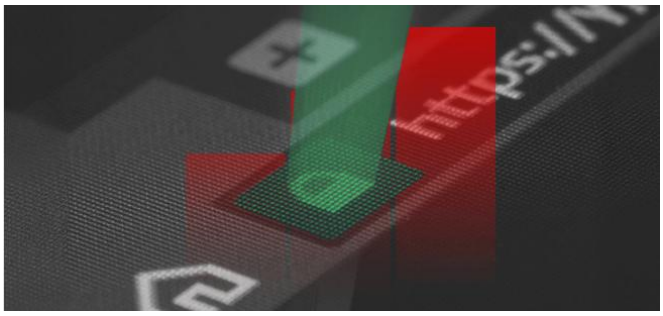
# Boletín de Ciberseguridad

## Riesgo de vulnerabilidades IT y OT

Enero - 2026

### Alertas de Ciberseguridad

*Extensiones maliciosas en Chrome Web Store roban credenciales de usuarios*



Descripción de la amenaza:

Investigadores de ciberseguridad identificaron en la tienda oficial de Google Chrome dos extensiones llamadas “Phantom Shuttle” que aparentan ser herramientas legítimas para pruebas de conexión y uso de proxy. Sin embargo, estas extensiones contienen código oculto que intercepta el tráfico web de los usuarios y roba información sensible, como contraseñas, datos de tarjetas o cookies de sesión. Una vez instaladas, las extensiones podían monitorear la actividad del navegador, capturar información ingresada en formularios web y enviar estos datos a servidores controlados por los atacantes, sin que el usuario lo notara.

Impacto

- Robo de credenciales, tokens de sesión y otros datos personales de usuarios que instalan estas extensiones.
- Acceso no autorizado a cuentas personales y empresariales.
- Afectación potencial a empleados que utilizan Google Chrome como navegador principal en el entorno laboral.

Riesgo

- Alto riesgo para empresas y usuarios que instalen extensiones desconocidas o con permisos excesivos, ya que pueden implicar exposición de credenciales o acceso a datos sensibles.
- Posibles daños operativos, reputacionales y financieros si cuentas corporativas son comprometidas.
- Las credenciales robadas pueden ser reutilizadas para ataques más graves, como accesos a redes empresariales o campañas de fraude.

Recomendaciones

- Implementar políticas corporativas de uso de navegadores y extensiones en entornos empresariales.
- Exigir controles centralizados de navegación para usuarios corporativos.
- Considerar el factor humano dentro de los indicadores de riesgo de ciberseguridad.

***La amenaza creciente de phishing móvil usando PDFs***


Descripción de la amenaza

Investigadores de Zimperium reportaron un aumento en campañas de phishing móvil o Mishing que utilizan archivos PDF como medio principal de engaño. Los atacantes envían estos documentos mediante SMS o aplicaciones de mensajería, simulando ser facturas, notificaciones o comprobantes legítimos. Dentro del PDF se incluyen enlaces o botones falsificados que redirigen a páginas diseñadas para robar credenciales o información sensible.
El uso de PDFs incrementa la efectividad del ataque, ya que en dispositivos móviles la vista previa oculta detalles importantes y genera mayor confianza en el usuario. Además, esta técnica evade muchos controles tradicionales, que no analizan de forma profunda los archivos recibidos vía mensajería móvil, convirtiéndolos en un vector discreto y cada vez más utilizado.

Impacto

- Robo de credenciales bancarias, corporativas o personales.
- Compromiso de cuentas por accesos no autorizados.
- Incremento de ataques dirigidos al aprovechar la ingeniería social en móviles.
- Evade controles tradicionales que analizan solo enlaces o adjuntos en correos.

Riesgo

- Alto, debido a suplantación convincente y carácter móvil.
- Creciente superficie de ataque no cubierta por controles clásicos de correo y red.
- Dificultad de detección temprana, aumentando el tiempo de permanencia del atacante.

- Impacto directo en ejecutivos y personal clave, que suelen usar el móvil como principal herramienta.

Recomendaciones

- Invertir en ciberseguridad en dispositivos móviles con capacidad de análisis de PDFs, enlaces y comportamiento.
- Actualizar los programas de concientización, incorporando escenarios reales de mishing orientados a ejecutivos.
- Definir lineamientos claros de uso de dispositivos móviles para acceso a información corporativa.