PHISHING

Análisis de la Técnica de Ataque T1566

1 Definición

Técnica de ingeniería social donde un atacante se hace pasar por alguien legítimo para engañar a la víctima y robar información o instalar malware a través de medios electrónicos.

2 Modalidades del Ataque

Spearphishing Attachment
- Archivo adjunto malicioso.
- **Objetivo:** Instalar malware.

Spearphishing Via Service
- Enlace a sitio falso.
- **Objetivo:** Robar credenciales.

Spearphishing Link
- Mensaje por red social o plataforma.
- **Objetivo:** Engaño directo.

Spearphishing Voice
- Llamada engañosa.
- **Objetivo:** Obtener info.

3 Sección de defensa

MITIGACIÓN : Cómo Prevenirlo

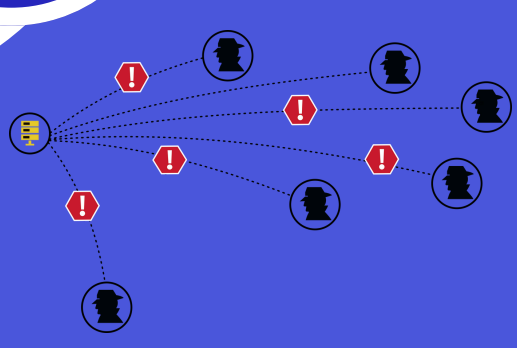
🛡️ **Protección**
- 🎓 ***Capacitación***: Enseñar a reconocer amenazas.
- ✉️ ***Filtros de Correo***: Bloqueo automático.
- 🔐 ***MFA***: Una barrera extra.
- 💻 ***Aislamiento*** : Ejecutar en entornos seguros.

DETECCIÓN : Cómo Descubrirlo

🔍 Detección
- 🌐 ***Monitoreo de Red***:Vigilar tráfico sospechoso.
- 📄 ***Análisis de Archivos***:Buscar actividad anómala.
- 🔎 ***Inspección de Contenido***:Analizar correos y logs.
- 🗣️ ***Reporte de Usuarios***: Fomentar la colaboración.

4 Conclusión

Es una amenaza persistente y efectiva porque explota la confianza humana.
No se limita a usuarios inexpertos. La mejor defensa es una combinación de escepticismo y educación: cultura no trust.
La prevención y la concienciación son clave para protegerse.



5 Caso de ejemplo

El fraude a Google y Facebook (2013-2015)
Se hizo pasar por un gran fabricante de hardware asiático y envió facturas falsas a Google y Facebook. Mediante correos electrónicos de phishing muy bien elaborados, engañó a los departamentos de contabilidad de ambas compañías para que le transfirieran más de 100 millones de dólares a sus cuentas