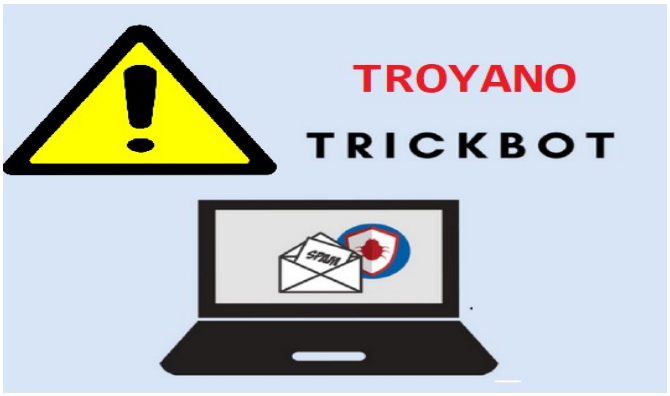
ALERTA: TROYANO TRICKBOT (02/NOVIEMBRE/2021)



Varios centros de respuesta a incidentes informáticos habrían detectado actividad maliciosa del troyano TRICKBOT, enfrentando así un alto riesgo de comprometimiento de sistemas de información.

Introducción

TRICKBOT en un troyano sofisticado que es propagado por ciber atacantes a través de campañas de spear phishing, las cuales tienen un alto nivel de personalización para atacar al objetito, orientándolo hacia enlaces para descarga del troyano. Las características técnicas del troyano TRICKBOT están orientadas hacia la captura pasiva y activa de información sensible tales como credenciales de acceso a sistemas de información.

Dentro de las principales amenazas que genera TRICKBOT son las siguientes:

1. Infectar sistemas con los ransowmare Ryuk y Conti.
2. Operar como descargador de archivos maliciosos para Emotet.

Respecto del Troyano TRICKBOT, MITRE señala que se han identificado 47 técnicas de ataque dentro 8 categorías de seguridad, siendo de las más importantes las de Escalamiento de Privilegios y Evasión Defensiva de detección.

Vector de ataque:

- TrickBot ha utilizado un correo electrónico con una hoja de Excel que contiene una macro maliciosa para implementar el malware.

- Las víctimas de TrickBot descargan sin saberlo un archivo JavaScript malicioso que, cuando se abre, se comunica automáticamente con el servidor C2 del actor malicioso para descargar TrickBot en el sistema de la víctima.
- TrickBot se ha enviado a través de enlaces maliciosos en correos electrónicos de phishing o spearphishing en un intento de atraer a los usuarios para que hagan clic en un enlace malicioso.

En consideración alto riesgo contra la confidencialidad, integridad y disponibilidad de los activos de información que pudiesen ser afectados por el troyano TRICKBOT, el EcuCERT de ARCOTEL recomienda a su comunidad objetivo, tomar en consideración las siguientes recomendaciones:

1. Bloquear conexiones de direcciones IP consideradas como sospechosas o inusuales.

2. Instalar y actualizar los programas antivirus utilizados para la protección de la red.

3. Implementar acciones de control a fin de identificar conexiones atípicas hacia la red organizacional protegida.

4. Realizar ejercicios de capacitación de ingeniería social y phishing.

Referencias

- US CERT CISA (2021). TrickBot Malware, Alert (AA21-076A). Disponible en https://us-cert.cisa.gov/ncas/alerts/aa21-076a

- US CERT CISA (2021). Fact Sheet: TrickBot Malware. Disponible en https://us-cert.cisa.gov/sites/default/files/publications/TrickBot_Fact_Sheet_508.pdf