	EC-2022-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	03-marzo-2022	**Malware QakBot**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Código Malicioso
Nivel de riesgo: Alta

II. ALERTA

QackBot (QakBot, Quakbot, Pinkslipbot) es un malware que se identificó por primera vez en el 2007 y que desde el 2021 se expandió rápidamente; robando información del navegador y de los correos electrónicos de las víctimas.

Figura 1. Ilustración asociada a QakBot

III. INTRODUCCIÓN

Un malware es una combinación de dos palabras: ***malicioso*** y ***software***; este término describe cualquier forma de código malicioso independientemente de cómo afecte a las víctimas, cómo se comporte o el daño que cause.

En este sentido, el malware QackBot es un troyano bancario y ladrón de información que los ciberdelincuentes han estado usando desde 2007 y que desde el 2021 ha vuelto con vigencia y según varios reportes de analistas de seguridad, se demora 30 minutos en robar datos confidenciales y 50 minutos en saltar a una estación de trabajo adyacente.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

	EC-2022-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	03-marzo-2022	**Malware QakBot**	V 1.1

IV. VECTOR DE ATAQUE: Remoto

Las investigaciones realizadas señalan que QakBot emplea campañas de correo electrónico malicioso para entregar un documento Excel (xls); al momento de abrir este archivo, el cargador DLL inicial de QakBot (con una extensión html para no ser detectado) se descarga y se almacena en el disco duro, una vez ejecutado se crea una tarea programada para elevarse al sistema.

En la siguiente gráfica se observa la manera de distribución del malware.

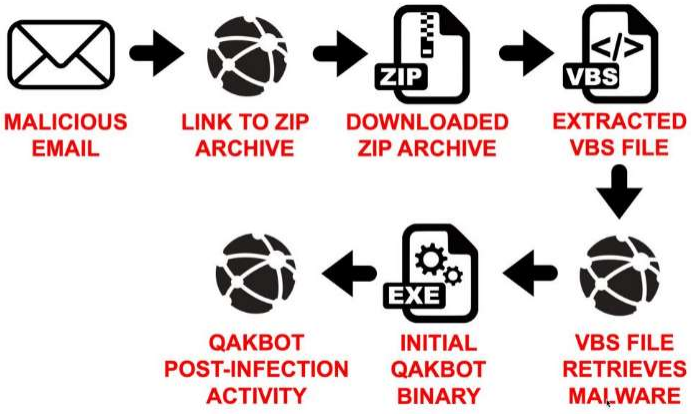

Figura 2. Ilustración asociada a distribución de QakBot

En la siguiente gráfica se observa una imagen asociada a un correo electrónico malicioso que tiene como adjunto a QakBot.

	EC-2022-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	03-marzo-2022	**Malware QakBot**	V 1.1

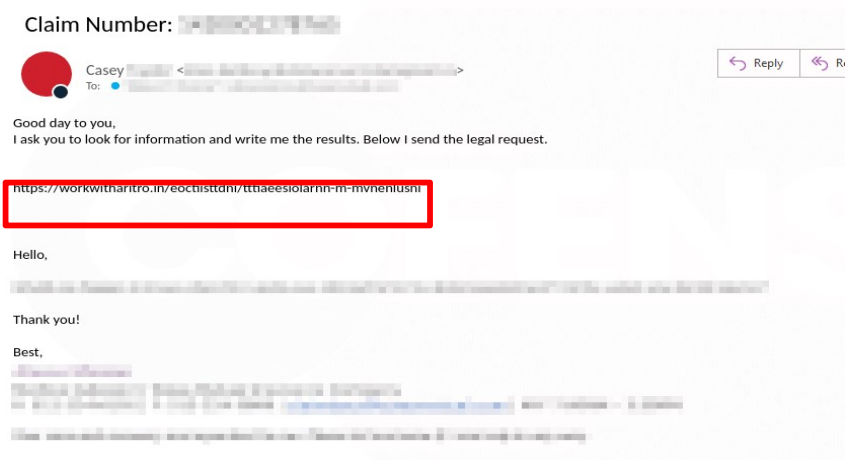

Figura 1. Ilustración asociada a correo malicioso
Fuente: Cofense

Dando clic en la URL maliciosa, se descarga un ZIP con el mismo nombre que la última parte de la ruta de la URL y dentro de este archivo ZIP se encuentra un archivo XLS.

En la siguiente gráfica se observa se observa el archivo Excel.

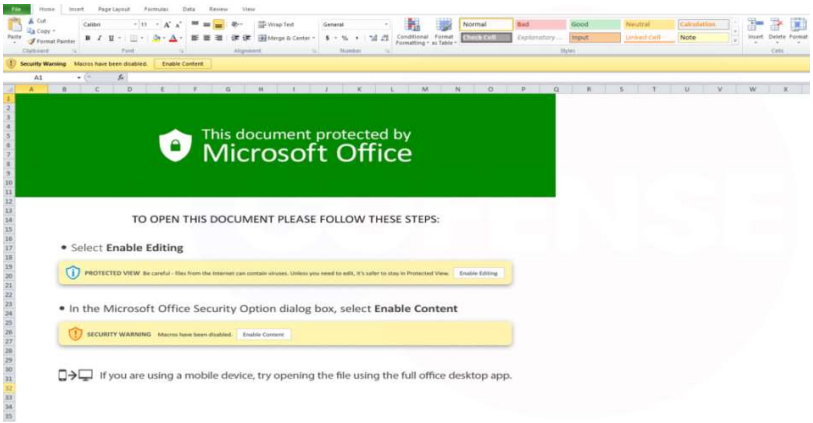

Figura 1. Ilustración asociada a archivo Excel malicioso
Fuente: Cofense

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

	EC-2022-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	03-marzo-2022	**Malware QakBot**	V 1.1

Los investigadores señalan que Qbot también robará las credenciales de Windows al volcar la memoria del proceso LSASS (Servicio de servidor de autoridad de seguridad local) y al robarlas de los navegadores web. Estas credenciales se pueden usar para propagarse lateralmente a otros dispositivos en la red.

V. INDICADORES DE COMPROMISO

A continuación se mencionan los indicadores de compromiso asociados a QakBot.

Ítem	Descripción de indicador	
Red	120.150.218.241:995 71.74.12.34:443 24.229.150.54:995 185.250.148.74:443 136.232.34.70:443 82.77.137.101:995 75.188.35.168:443 72.252.201.69:443 109.12.111.14:443 68.204.7.158:443 196.218.227.241:995 27.223.92.142:995 76.25.142.196:443 73.151.236.31:443	185.250.148.74:2222 173.21.10.71:2222 189.210.115.207:443 105.198.236.99:443 47.22.148.6:443 24.55.112.61:443 24.139.72.117:443 45.46.53.140:2222 92.59.35.196:2222 95.77.223.148:443 68.186.192.69:443 89.101.97.139:443 173.25.166.81:443 140.82.49.12:443
URL para el archivo zip inicial	hxxps://prajoon.000webhostapp[.]com/wp-content/uploads/2019/12/last/033/033.zip hxxps://psi-uae[.]com/wp-content/uploads/2019/12/last/870853.zip hxxps://re365[.]com/wp-content/uploads/2019/12/last/85944289/85944289.zip hxxps://liputanforex.web[.]id/wp-content/uploads/2019/12/last/794/794.zip hxxp://eps.icothanglong.edu[.]vn/forward/13078.zip hxxp://hitechrobo[.]com/wp-content/uploads/2020/01/ahead/84296848/84296848.zip hxxp://faithoasis.000webhostapp.com/wp-content/uploads/2020/01/ahead/550889.zip hxxps://madisonclubbar[.]com/fast/invoice049740.zip hxxp://zhinengbao[.]wang/wp-content/uploads/2020/01/lane/00571.zip hxxp://bhatner[.]com/wp-content/uploads/2020/01/ahead/9312.zip hxxp://santedeplus[.]info/wp-content/uploads/2020/02/ending/1582820/1582820.zip	

Tabla 1. IOC asociados a QakBot

En referencia al Impacto que produce este malware, no se observaron las acciones finales del actor de amenazas; sin embargo, los datos extraídos de la red podrían usarse para realizar más ataques o venderse a terceros.

	EC-2022-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	03-marzo-2022	**Malware QakBot**	V 1.1

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución.
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Tener actualizado y utilizar, un software anti-virus
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.

VII. REFERENCIAS:

Bill, T. (08 de 02 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/qbot-needs-only-30-minutes-to-steal-your-credentials-emails/

ESET. (s.f.). *ESET*. Obtenido de ESET: https://www.eset.com/es/caracteristicas/malware/#

Kat, G., & Kirk, K. (24 de 02 de 2022). *Centro de Defensa contra el Phishing de Cofense*. Obtenido de Centro de Defensa contra el Phishing de Cofense: https://cofense.com/blog/qakbot-campaign-attempts-to-revive-old-emails

Thedfirreport. (07 de 02 de 2022). *Thedfirreport*. Obtenido de Thedfirreport: https://thedfirreport.com/2022/02/07/qbot-likes-to-move-it-move-it/

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec