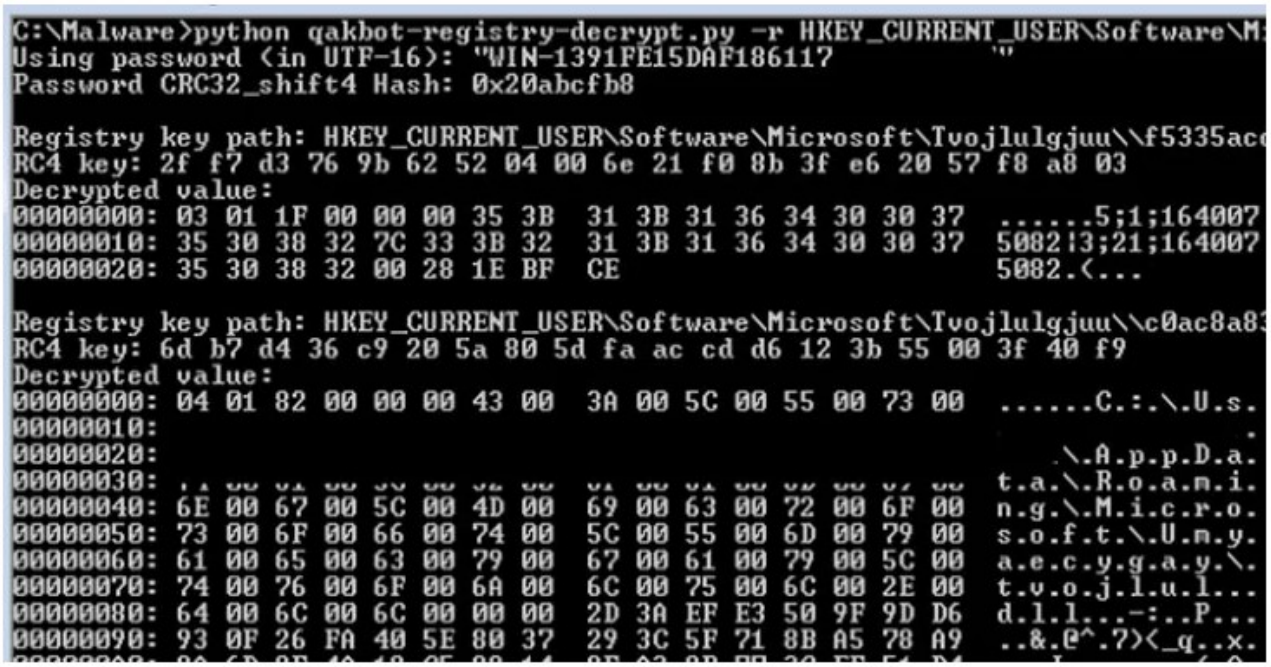
Investigadores logran descifrar las claves de registro del troyano bancario Quakbot

Autor: I. Stepanenko

Fecha: Monday 24th of January 2022 09:55:23 AM



Investigadores de seguridad cibernética descifraron el mecanismo por el cual el versátil troyano bancario Quakbot maneja la inserción de datos de configuración encriptados en el Registro de Windows.

Quakbot, también conocido como QBot, QuackBot y Pinkslipbot, ha sido observado en la naturaleza desde 2007. Aunque se diseñó principalmente como un malware para robar información, Quakbot cambió sus objetivos y adquirió una nueva funcionalidad para ofrecer plataformas de ataque posteriores al compromiso como Cobalt Strike Beacon, con el objetivo final de cargar ransomware en las máquinas infectadas.

> «Se ha desarrollado continuamente, con nuevas capacidades introducidas, como el movimiento lateral, la capacidad de filtrar correo electrónico y datos del navegador, y de instalar malware adicional», dijeron los investigadores de Trustwave Lloyd Macrohon y Rodel Mendrez.

En los últimos meses, las campañas de phishing culminaron con la distribución de un nuevo

cargador llamado SQUIRRELWAFFLE, que actúa como un canal para recuperar las cargas útiles de la etapa final, como Cobalt Strike y QBot.

Las versiones más nuevas de Quakbot, también tienen la capacidad de secuestrar datos de correo electrónico y navegador, así como insertar información de configuración cifrada relacionada con el malware en el registro en lugar de escribirla en un archivo en el disco como parte de sus intentos de no dejar rastro de la infección.

> «Aunque QuakBot no se está volviendo completamente sin archivos, sus nuevas tácticas seguramente reducirán su detección», dijeron los investigadores de Hornetsecurity en diciembre de 2020.

El análisis de Trustwave en el malware tiene como objetivo realizar ingeniería inversa en este proceso y descifrar la configuración almacenada en la clave de registro, y la compañía de seguridad cibernética dijo que la clave utilizada para cifrar los datos del valor de la clave de registro se deriva de una combinación de nombre de computadora, número de serie del volúmen, y el nombre de la cuenta de usuario, que luego se codifica y saltea junto con un identificador (ID) de un byte.

«El resultado del hash SHA1 se utilizará como una clave derivada para descifrar los datos del valor de la clave de registro correspondiente al ID usando el algoritmo RC4», dijeron los investigadores, además de poner a disposición una utilidad de descifrado basada en Python que se puede usar para extraer la configuración desde el registro.