Una campaña de botnet aumentó su actividad durante el último mes, con piratas informáticos que la utilizan para distribuir ransomware y otras piezas de malware.

Los investigadores de Check Point analizaron las amenazas cibernéticas más comunes dirigidas a las organizaciones para su informe malware más buscado de junio de 2020, y vieron un gran aumento en los ataques por medio de la botnet Phorpiex.

Phorpiex es conocida por distribuir una serie de campañas de malware y spam, incluyendo campañas de correo electrónico de distorsión a gran escala, pero en el transcurso de junio, la cantidad de detecciones aumentó de forma significativa en comparación con mayo.

El aumento en las detecciones de Phorpiex creció al punto de ser la segunda campaña de malware más detectada durante junio, después de haber sido clasificada el 13 de mayo. El número de intentos de ataque fue tan alto que el 2 por ciento de las organizaciones fueron atacadas por esta botnet.

La botnet envía correos electrónicos no deseados que intentan entregar una carga maliciosa. Durante el último mes, se utilizó para impulsar una campaña del ransomware Avaddon.

Esta familia de ransomware en particula, solo apareció en junio y Phorpiex intenta atraer a las víctimas para que abran un archivo adjunto zip en un correo electrónico de phishing que utiliza un emoji de guiño.

Anteriormente, Phorpiex, también conocido como Trik, se ha utilizado para distribuir campañas de spam para otras formas de ransomware, incluidos GrandCrab y Pony, además de la extracción de criptomonedas en máquinas infectadas.

> *«Las organizaciones deberían educar a los empleados sobre cómo identificar los tipos de correo no deseado que conllevan estas amenazas, como la última campaña dirigida a los usuarios con correos electrónicos que contienen un emoji de guiño y asegurando que implementen seguridad que les impide activamente infectar sus*

> *redes»*, dijeron los investigadores de Check Point.

Aunque los ataques de Phorpiex aumentaron de forma significativa, el malware más comúnmente detectado durante junio fue Agent Tesla, un troyano de acceso remoto avanzado que fue detectado dirigido al 3% de las organizaciones.

Agent Tesla es un ladrón de información que emplea un keylogger, brinda a los atacantes la capacidad de ver absolutamente todo en la computadora infectada, incluidos los nombres de usuario, contraseñas, historial de navegador, información del sistema, entre otra información.

El tercer malware más detectado en junio fue XMRig, un malware de minería de criptomonedas de código abierto, que utiliza la potencia de la CPU de las máquinas infectadas para generar la criptomoneda Monero. Este malware ha estado activo desde 2017.

El resto del top 10 de malware más buscado para junio se compone de nombres conocidos como Dridex, Trickbot, Ramnit y Emotet, que por mucho tiempo fueron elementos básicos de la actividad de piratería, ya sea mediante el robo de información o siendo utilizados para campañas más destructivas.