# ALERTA

## Distribución de Malware Función Quick Assist de Microsoft

[COLCERT AL-0528-027]

TLP:CLEAR


**"Quick Assist es una herramienta legítima de Windows que puede ser afectada por esta amenaza"**

Cibercriminales usan Quick Assist (herramienta legítima de Microsoft) para engañar y desplegar ransomware Black Basta. Se hacen pasar por soporte técnico para ganar acceso remoto.

### Contexto

Quick Assist, una herramienta de Microsoft para Asistencia rápida, la cual permite compartir dispositivos Windows o macOS con otra persona a través de una conexión remota. El grupo criminal Storm-1811 está explotando esta función para distribuir el ransomware Black Basta. Los atacantes utilizan técnicas de ingeniería social, como la suplantación de identidad de soporte técnico de Microsoft, para engañar a las víctimas a fin de que instalen software remoto de monitoreo (RAT).

### Detalles de la Amenaza

**Vector de ataque:** Ingeniería social, suplantación de identidad de soporte técnico de Microsoft.
**Payload:** Black Basta ransomware, QakBot, Cobalt Strike.
**Herramienta utilizada:** Quick Assist (legítima de Microsoft).
**Objetivo:** Robo de datos, cifrado de archivos.

### Para protegerse contra estas vulnerabilidades

**Deshabilitar o desinstalar Quick Assist:** Si no se utiliza habitualmente, elimine esta herramienta para reducir la superficie de ataque.
**Fortalecer la autenticación:** Implementar MFA (multifactor authentication)
**Concientizar a los empleados.**
**Soluciones de seguridad:** Implementar antivirus, anti-malware y firewalls actualizados.
**Copias de seguridad regulares.**

**Es importante que los usuarios apliquen las actualizaciones de seguridad lo antes posible y tomen medidas para mitigar el riesgo de explotación**

**NIVEL DE RIESGO**

**ALTO**

**FUENTES:**

https://www.microsoft.com/en-us/msrc
https://www.bleepingcomputer.com/news/security/black-basta-bl00dy-ransomware-gangs-join-screenconnect-attacks/
https://www.cisa.gov/stopransomware/ransomware-101

COLCERT