Los expertos en seguridad informática han descubierto una nueva operación que está aprovechando una vulnerabilidad de seguridad recientemente divulgada en los dispositivos Fortinet FortiClient EMS para distribuir cargas útiles de ScreenConnect y Metasploit Powerfun.

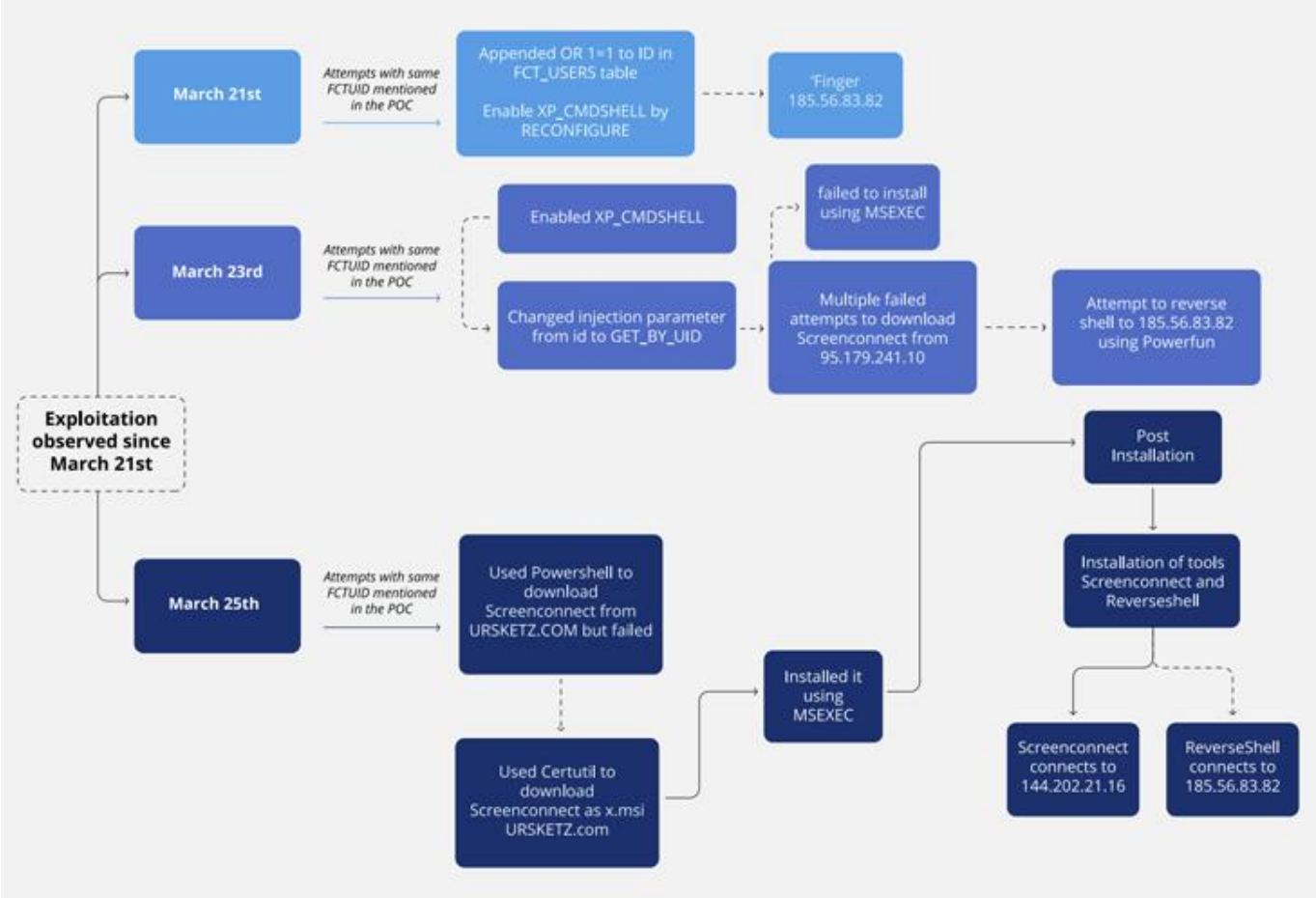
Esta actividad implica la explotación de la CVE-2023-48788 (puntuación CVSS: 9.3), una falla crítica de inyección SQL que podría permitir a un atacante no autorizado ejecutar código o comandos no autorizados mediante solicitudes especialmente diseñadas.

La empresa de seguridad cibernética Forescout está siguiendo de cerca la operación bajo el nombre en clave Connect:fun debido al uso de ScreenConnect y Powerfun para actividades posteriores a la explotación.

El objetivo de la intrusión fue una empresa de medios no identificada que tenía su dispositivo FortiClient EMS vulnerable expuesto en Internet poco después de que se publicara un exploit de prueba de concepto (PoC) para la vulnerabilidad el 21 de marzo de 2024.

En los días siguientes, se observó que el adversario desconocido intentaba aprovechar la vulnerabilidad para descargar sin éxito ScreenConnect y luego instalar el software de escritorio remoto utilizando la utilidad msiexec.

Sin embargo, el 25 de marzo, el exploit de PoC se utilizó para ejecutar código PowerShell que descargó el script Powerfun de Metasploit e inició una conexión inversa a otra dirección IP.



También se detectaron declaraciones SQL diseñadas para descargar ScreenConnect desde un dominio remoto («ursketz[.]com») utilizando certutil, que luego se instaló a través de msiexec antes de establecer conexiones con un servidor de comando y control (C2).

Hay evidencia que sugiere que el actor de amenazas detrás de esta operación ha estado activo desde al menos 2022, centrando su atención específicamente en los dispositivos Fortinet y utilizando los idiomas vietnamita y alemán en su infraestructura.

> *«La actividad observada claramente implica un componente manual, como lo demuestran todos los intentos fallidos de descargar e instalar herramientas, así*

> *como el tiempo relativamente largo entre los intentos»*, dijo el investigador de seguridad Sai Molige.
>
> *«Esto indica que esta actividad forma parte de una campaña específica, en lugar de un exploit incluido en botnets cibernéticas automatizadas. Según nuestras observaciones, parece que los actores detrás de esta operación no están llevando a cabo escaneos masivos, sino que están seleccionando entornos objetivo que tienen dispositivos VPN».*

Forescout señaló que este ataque comparte similitudes tácticas e infraestructurales con otros incidentes documentados por Palo Alto Networks Unit 42 y Blumira en marzo de 2024 que involucran el abuso de la CVE-2023-48788 para descargar ScreenConnect y Atera.

Se recomienda a las organizaciones que apliquen los parches proporcionados por Fortinet para mitigar posibles amenazas, supervisen el tráfico sospechoso y utilicen un cortafuegos de aplicaciones web (WAF) para bloquear solicitudes potencialmente maliciosas.