Una vulnerabilidad crítica de seguridad en el software de videoconferencias TrueConf ha sido explotada activamente como un ataque de día cero, en el marco de una campaña dirigida a entidades gubernamentales en el sudeste asiático, conocida como TrueChaos.

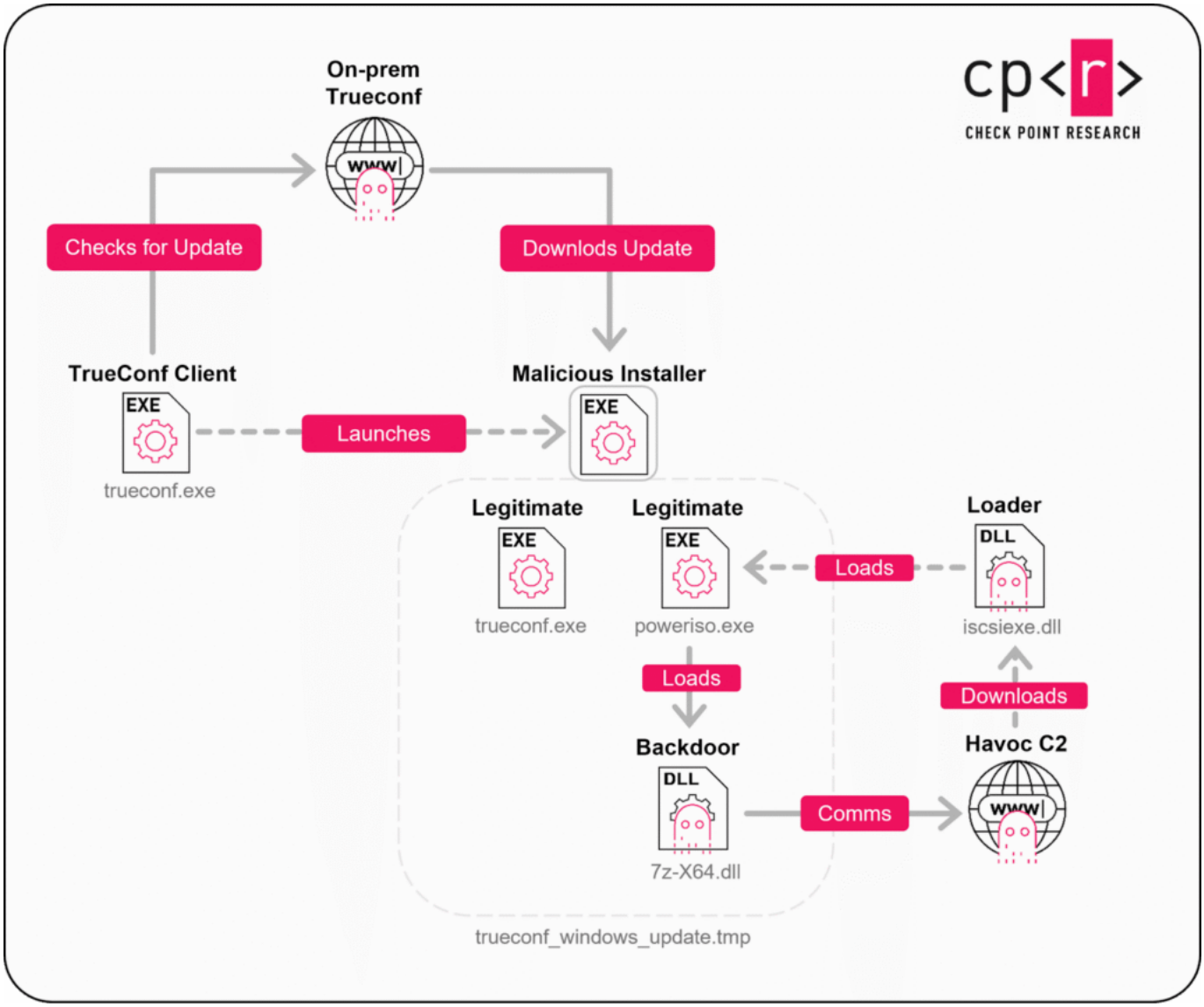
La falla identificada como CVE-2026-3502 (con una puntuación CVSS de 7.8) radica en la ausencia de verificación de integridad al descargar actualizaciones de la aplicación, lo que permite a un atacante distribuir versiones manipuladas y provocar la ejecución de código arbitrario. Este problema ya fue corregido en el cliente de TrueConf para Windows a partir de la versión 8.5.3, publicada a inicios de este mes.

«La vulnerabilidad se origina en el uso indebido del mecanismo de validación del actualizador de TrueConf, lo que posibilita que un atacante con control sobre el servidor local de TrueConf distribuya y ejecute archivos arbitrarios en todos los dispositivos conectados,» señaló Check Point en un informe difundido hoy.

En términos más simples, si un atacante logra tomar el control del servidor local de TrueConf, puede reemplazar el paquete de actualización por una versión comprometida. Esta es descargada automáticamente por las aplicaciones cliente instaladas en los dispositivos de los usuarios, debido a la falta de validaciones suficientes que garanticen la autenticidad del contenido proporcionado por el servidor.

Se ha detectado que la campaña TrueChaos aprovecha esta debilidad en el sistema de actualizaciones para desplegar probablemente el framework de comando y control (C2) de código abierto Havoc en los equipos vulnerables. La actividad ha sido atribuida con un nivel de confianza moderado a un actor de amenazas vinculado con China.

Los primeros ataques que explotaron esta vulnerabilidad fueron registrados a principios de 2026 por la compañía de ciberseguridad, aprovechando la confianza implícita del cliente en el mecanismo de actualización para distribuir un instalador malicioso. Este, a su vez, utiliza la técnica de carga lateral de DLL (DLL side-loading) para ejecutar una puerta trasera.



El componente malicioso en forma de DLL («7z-x64.dll») también ha mostrado ejecutar acciones manuales para llevar a cabo reconocimiento, establecer persistencia y descargar cargas adicionales («iscsiexe.dll») desde un servidor FTP («47.237.15[.]197»). El propósito principal de «iscsiexe.dll» es asegurar la ejecución de un binario aparentemente legítimo («poweriso.exe»), que se utiliza para cargar la puerta trasera de forma encubierta.

Aunque no se ha determinado con certeza el malware final desplegado en la última fase del

ataque, se considera altamente probable que el objetivo sea instalar el implante Havoc.

La relación de TrueChaos con un actor vinculado a China se sustenta en las tácticas observadas, como el uso de carga lateral de DLL, así como el empleo de infraestructuras de comando y control alojadas en Alibaba Cloud y Tencent. Además, la misma víctima fue atacada en el mismo periodo mediante ShadowPad, una puerta trasera sofisticada ampliamente utilizada por grupos de hacking asociados a China.

Asimismo, el uso de Havoc ha sido relacionado con otro actor chino denominado Amaranth-Dragon, en ataques dirigidos a organismos gubernamentales y fuerzas del orden en el sudeste asiático durante 2025.

«La explotación de CVE-2026-3502 no requería que el atacante comprometiera cada dispositivo de manera individual,» indicó Check Point. *«En su lugar, el atacante aprovechó la relación de confianza entre el servidor local central de TrueConf y sus clientes. Al sustituir una actualización legítima por una maliciosa, convirtió el proceso habitual de actualización del producto en un canal de distribución de malware a través de múltiples redes gubernamentales conectadas.»*