El grupo de amenazas vinculado a Corea del Norte, conocido como el Grupo Lazarus, ha sido detectado explotando una vulnerabilidad crítica que ya ha sido solucionada y que afecta a Zoho ManageEngine ServiceDesk Plus. Esto se hace con el propósito de distribuir un troyano de acceso remoto llamado QuiteRAT.

Los objetivos de estos ataques incluyen infraestructuras esenciales de Internet y entidades relacionadas con la atención médica en Europa y los Estados Unidos. Estos hallazgos provienen de un análisis realizado por la empresa de ciberseguridad Cisco Talos y fueron publicados en dos partes hoy.

Además, al investigar más a fondo la infraestructura de ataque reciclada que este adversario utiliza en sus ataques a empresas, se ha descubierto una nueva amenaza a la que se le ha dado el nombre de CollectionRAT.

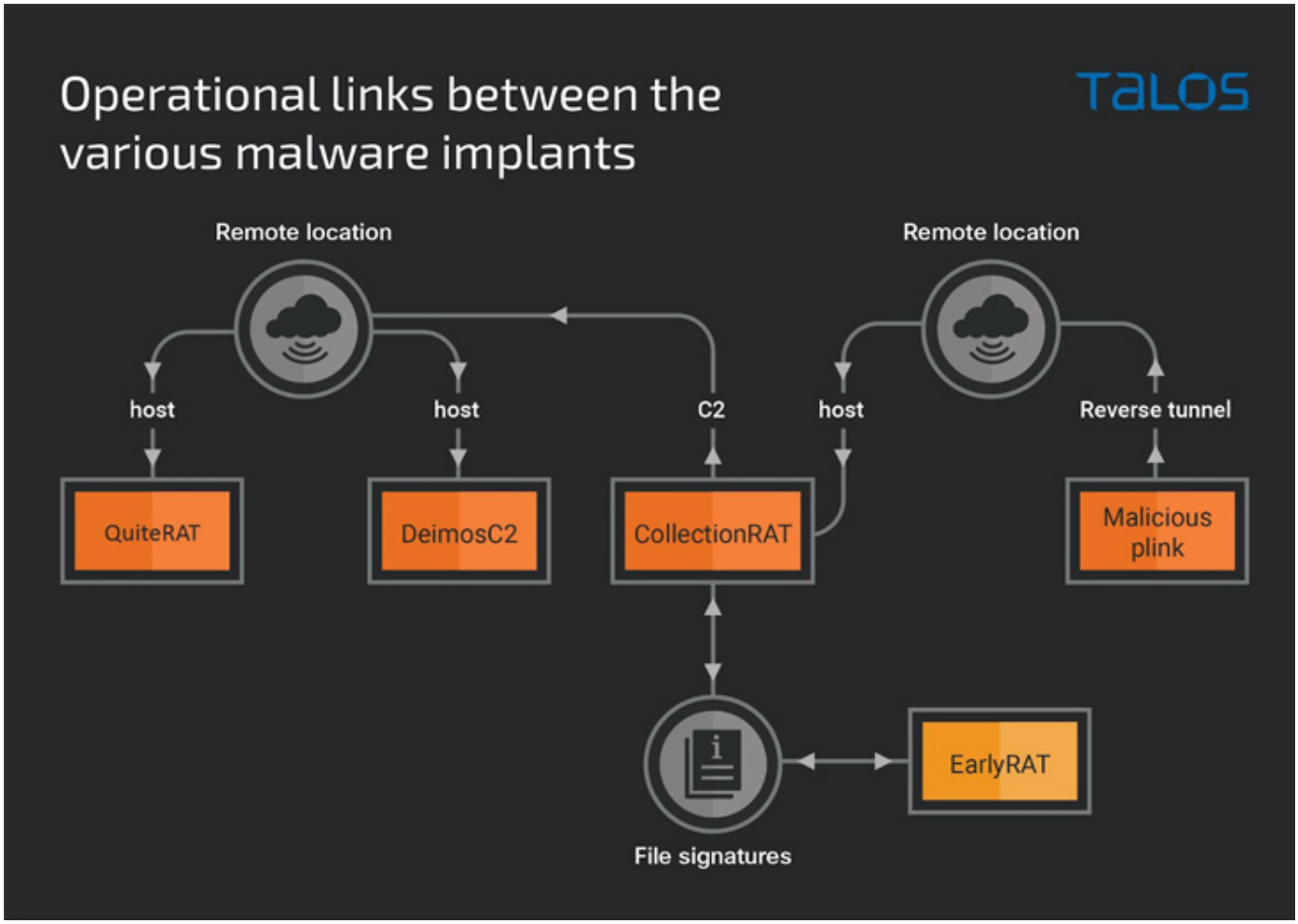
El hecho de que el Grupo Lazarus continúe utilizando las mismas tácticas a pesar de que estas han sido bien documentadas durante varios años, resalta la confianza que tienen en sus operaciones, según lo señalado por Talos.

Se dice que QuiteRAT es la evolución de MagicRAT y este último es, a su vez, una continuación de TigerRAT. Por otro lado, CollectionRAT parece compartir similitudes con EarlyRAT (también conocido como Jupiter), que es un programa implantado escrito en PureBasic y tiene la capacidad de ejecutar comandos en el dispositivo comprometido.

> Los investigadores de seguridad, Asheer Malhotra, Vitor Ventura y Jungsoo An, afirman que *«QuiteRAT tiene muchas de las mismas capacidades que el malware más conocido del Grupo Lazarus, MagicRAT, pero su tamaño de archivo es considerablemente menor. Ambos programas están construidos sobre el marco de Qt y tienen la capacidad de ejecutar comandos de forma arbitraria».*

El uso del marco de Qt parece ser un esfuerzo intencional por parte del adversario para dificultar el análisis de su código, ya que esto *«aumenta la complejidad del malware».*

Esta actividad, que fue detectada a principios de 2023, involucra la explotación de una vulnerabilidad conocida como CVE-2022-47966, tan solo cinco días después de que un concepto de prueba (PoC) para esta vulnerabilidad fuera publicado en línea. Esto permitió la distribución del archivo binario de QuiteRAT directamente desde una URL maliciosa.



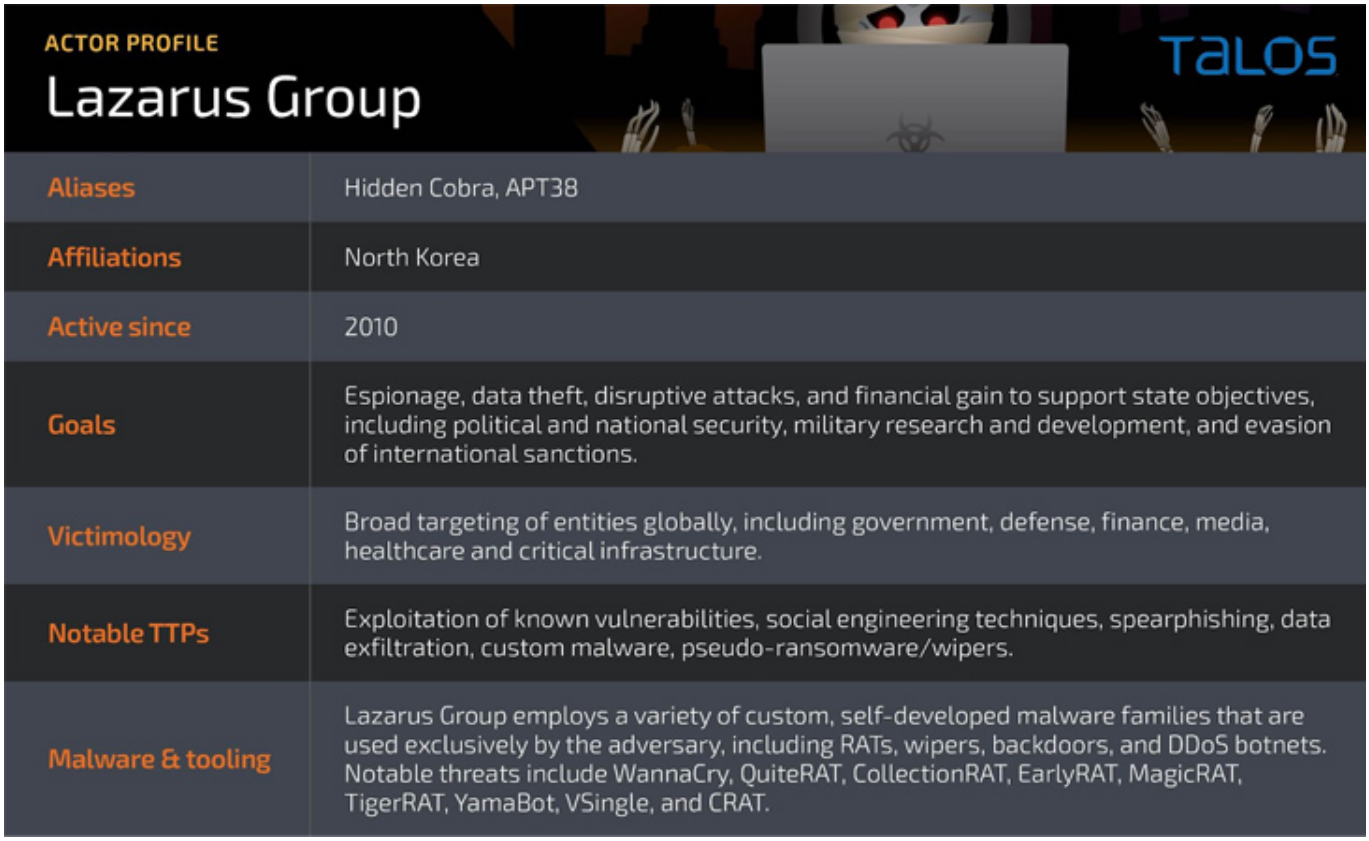
Los investigadores también destacan una diferencia clave entre MagicRAT y QuiteRAT, la cual es la falta de un mecanismo de persistencia incorporado en QuiteRAT. Esto significa que se necesita un comando del servidor para asegurar su funcionamiento continuo en el dispositivo comprometido.

Además, estos hallazgos se superponen con otra campaña de ciberataques que fue descubierta por WithSecure a principios de febrero. En esta campaña, se explotaron fallas de seguridad en dispositivos Zimbra no parcheados para infiltrar sistemas de víctimas y finalmente instalar QuiteRAT.

Cisco Talos ha informado que el adversario está *«cada vez más recurriendo a herramientas y estructuras de código abierto en la fase de acceso inicial de sus ataques, en lugar de utilizarlas estrictamente en la fase posterior a la violación».*

Esto incluye el uso del marco DeimosC2 de código abierto basado en GoLang para obtener un acceso duradero, mientras que CollectionRAT se utiliza principalmente para recopilar metadatos, ejecutar comandos arbitrarios, administrar archivos en el sistema infectado y entregar cargas adicionales.

No está claro de inmediato cómo se propaga CollectionRAT, pero las pruebas indican que se está utilizando una versión alterada de la utilidad PuTTY Link (Plink) de código abierto alojada en la misma infraestructura para establecer un túnel remoto en el sistema y distribuir el malware.



> *«El Grupo Lazarus anteriormente dependía del uso de implantes personalizados como MagicRAT, VSingle, Dtrack y YamaBot como medio para obtener acceso inicial persistente en un sistema comprometido con éxito»,* señalaron los investigadores.

> *«Estos implantes se adaptaban luego para desplegar una variedad de herramientas de código abierto o de uso general para llevar a cabo una serie de actividades maliciosas en la red empresarial comprometida».*

Este desarrollo es una indicación de que el Grupo Lazarus continúa cambiando sus tácticas y ampliando su conjunto de herramientas maliciosas, al mismo tiempo que aprovecha las

vulnerabilidades recién reveladas en el software con efectos devastadores.