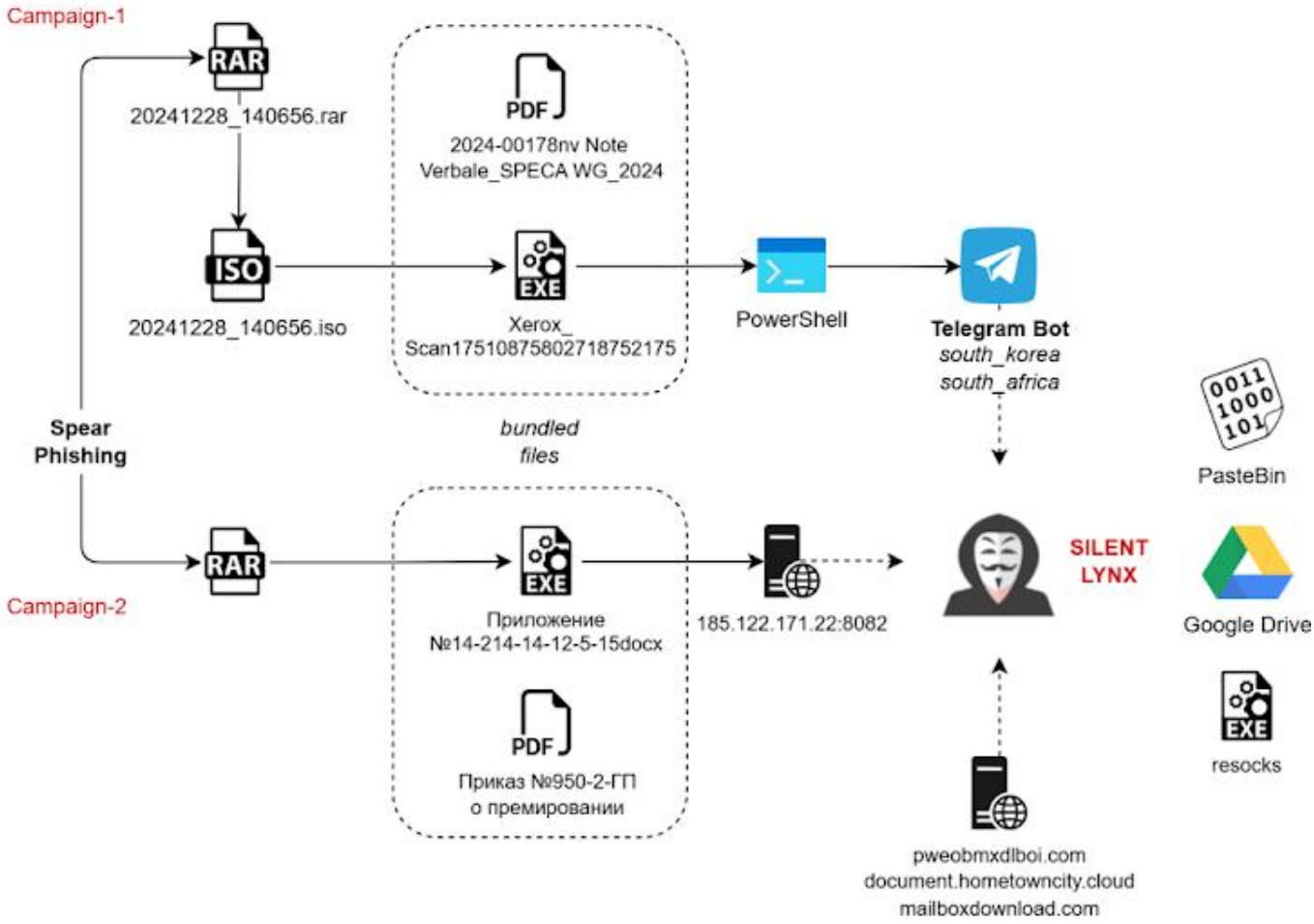
Un actor de amenazas previamente desconocido, denominado Silent Lynx, ha sido identificado como responsable de ciberataques dirigidos a diversas organizaciones en Kirguistán y Turkmenistán.

> *«Este grupo ha atacado anteriormente entidades en Europa del Este y centros de análisis gubernamentales en Asia Central relacionados con la toma de decisiones económicas y el sector financiero»,* explicó el investigador de Seqrite Labs, Subhajeet Singha, en un informe técnico publicado recientemente.

Entre los objetivos de este grupo de hackers se encuentran embajadas, abogados, bancos respaldados por el gobierno y centros de estudios estratégicos. La actividad ha sido atribuida, con un nivel de confianza moderado, a un actor de amenazas originario de Kazajistán.

El proceso de infección comienza con un correo de spear-phishing que incluye un archivo comprimido en formato RAR. Este archivo actúa como un mecanismo de entrega para programas maliciosos que permiten el acceso remoto a los sistemas comprometidos.

La primera de las dos campañas, detectada el 27 de diciembre de 2024 por la compañía de ciberseguridad, emplea el archivo RAR para desplegar un archivo ISO. Dentro de este se encuentra un ejecutable malicioso en C++ junto con un documento PDF señuelo. El programa ejecutable posteriormente activa un script de PowerShell que emplea bots de Telegram (denominados «@south_korea145_bot» y «@south_afr_angl_bot») para recibir órdenes y extraer información.



Entre las instrucciones ejecutadas mediante estos bots se encuentran comandos curl para descargar y almacenar archivos adicionales desde un servidor remoto («pweobmxdlboi[.]com») o desde Google Drive.

La segunda campaña, en cambio, utiliza un archivo RAR infectado que contiene un documento PDF engañoso y un ejecutable escrito en Golang. Este último está diseñado para establecer una conexión de acceso remoto con un servidor bajo control del atacante («185.122.171[.]22:8082»).

Seqrite Labs ha detectado ciertas similitudes estratégicas entre este actor de amenazas y

YoroTrooper (también conocido como SturgeonPhisher), un grupo vinculado a ataques dirigidos a países de la Comunidad de Estados Independientes (CIS) mediante el uso de herramientas basadas en PowerShell y Golang.

> *«Las operaciones de Silent Lynx evidencian una estrategia de ataque avanzada y compuesta por múltiples etapas, utilizando archivos ISO, cargadores en C++, scripts de PowerShell e implantes en Golang»*, destacó Singha.
>
> *«Su uso de bots de Telegram para el control de comandos, junto con documentos engañosos y un enfoque específico en ciertas regiones, subraya su interés en el espionaje en Asia Central y las naciones que forman parte de SPECA.»*