Los expertos en seguridad informática han descubierto una operación enfocada en atacar a Ucrania que se ha encontrado aprovechando una vulnerabilidad en Microsoft Office que tiene casi siete años de antigüedad, con el objetivo de instalar Cobalt Strike en sistemas comprometidos.

El proceso de ataque, que ocurrió a finales de 2023 según Deep Instinct, utiliza un archivo de presentación de PowerPoint («*signal-2023-12-20-160512.ppsx*«) como punto de inicio, lo cual sugiere que podría haberse compartido a través de la aplicación de mensajería instantánea Signal.

No obstante, no hay pruebas concretas que indiquen que el archivo PPSX se haya distribuido de esta manera, aunque el Equipo de Respuesta a Incidentes de Seguridad Informática de Ucrania (CERT-UA) ha descubierto dos campañas diferentes que utilizaron la aplicación de mensajería como vector para entregar malware en el pasado.

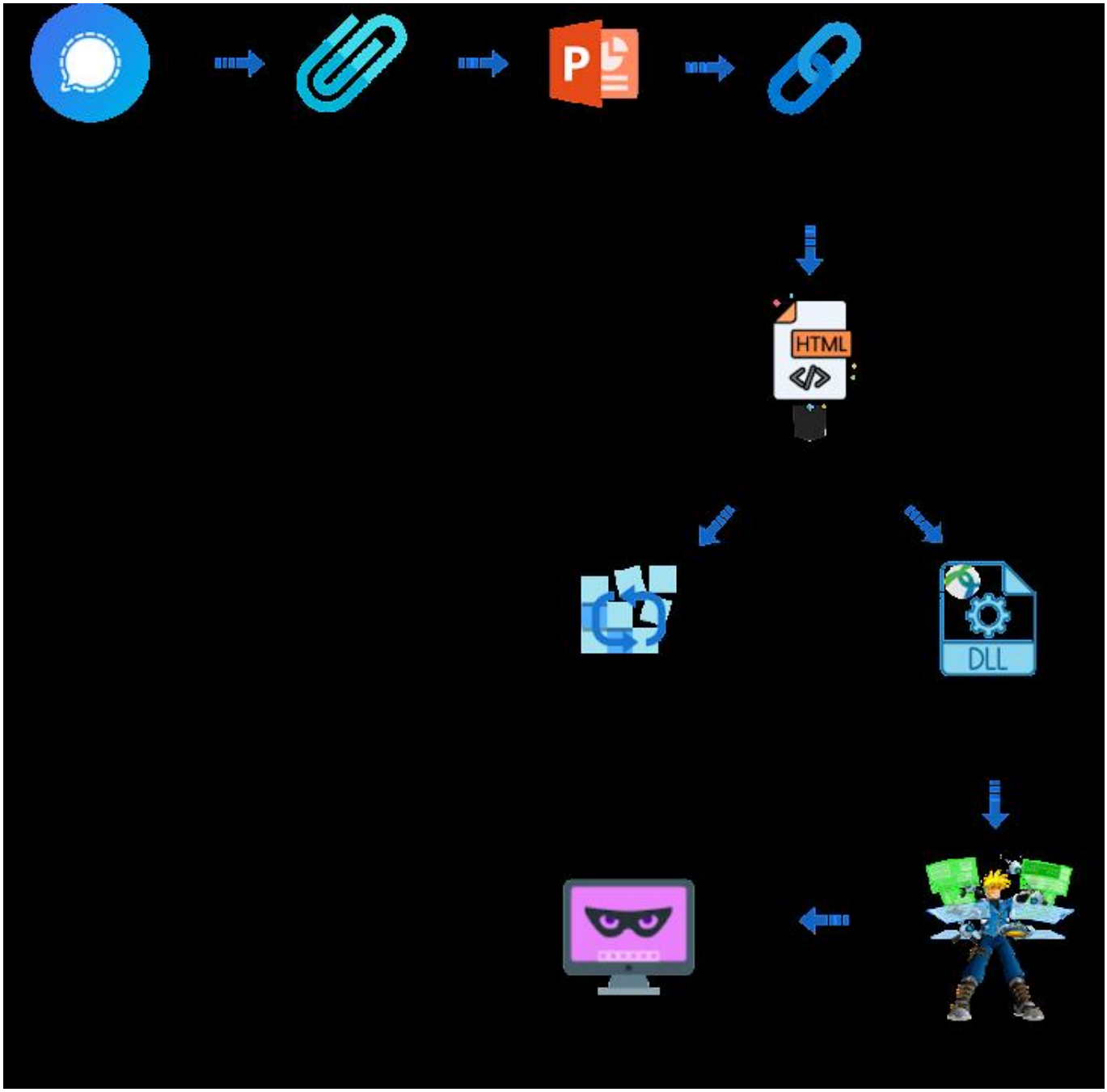
Recientemente, la agencia reveló que las fuerzas armadas ucranianas están siendo cada vez más blanco del grupo UAC-0184 a través de plataformas de mensajería y citas para distribuir malware como HijackLoader (también conocido como GHOSTPULSE y SHADOWLADDER), XWorm y Remcos RAT, así como programas de código abierto como sigtop y tusc para extraer datos de computadoras.

Según el investigador de seguridad Ivan Kosarev, *«El archivo PPSX (presentación de PowerPoint) parece ser un manual antiguo del Ejército de EE. UU. sobre cuchillas para limpiar minas (MCB) en tanques».* Kosarev también señaló que *«El archivo PPSX incluye un vínculo remoto con un objeto OLE externo»*.

Este proceso implica la explotación de CVE-2017-8570 (puntuación CVSS: 7.8), un fallo de ejecución remota de código que ya ha sido corregido en Office, el cual podría permitir a un atacante realizar acciones maliciosas al convencer a una víctima de abrir un archivo especialmente diseñado, para cargar un script remoto alojado en weavesilk[.]space.

El script altamente ofuscado posteriormente ejecuta un archivo HTML que contiene código

JavaScript, el cual establece persistencia en el host a través del Registro de Windows y descarga una carga útil adicional que se hace pasar por el cliente VPN Cisco AnyConnect.



El paquete contiene una biblioteca de enlaces dinámicos (DLL) que finalmente inserta un Beacon de Cobalt Strike alterado, una herramienta legítima de prueba de penetración, directamente en la memoria del sistema y espera instrucciones adicionales de un servidor de comando y control (C2) («petapixel[.]fun»).

La DLL también incluye funciones para verificar si se está ejecutando en una máquina virtual y evitar la detección por parte del software de seguridad.

Deep Instinct dijo que no pudo conectar los ataques a un actor o grupo de amenazas específico ni descartar la posibilidad de un ejercicio de red teaming. También es poco claro cuál es el objetivo final exacto de la intrusión.

> *«El anzuelo contenía contenido relacionado con lo militar, lo que sugiere que estaba dirigido al personal militar»,* dijo Kosarev.
>
> *«Pero los nombres de dominio weavesilk[.]space y petapixel[.]fun están camuflados como un sitio de arte generativo oscuro (weavesilk[.]com) y un sitio popular de fotografía (petapixel[.]com). Estos no están relacionados, y resulta un poco desconcertante por qué un atacante usaría estos específicamente para engañar al personal militar».*

La revelación llega después de que CERT-UA revelara que aproximadamente 20 proveedores de energía, agua y calefacción en Ucrania han sido atacados por un grupo patrocinado por el estado ruso llamado UAC-0133, un subgrupo dentro de Sandworm (también conocido como APT44, FROZENBARENTS, Seashell Blizzard, UAC-0002 y Voodoo Bear), que es responsable de la mayoría de todas las operaciones disruptivas y destructivas contra el país.

Los ataques, que tenían como objetivo sabotear operaciones críticas, implican el uso de malware como Kapeka (también conocido como ICYWELL, KnuckleTouch, QUEUESEED y wrongsens) y su variante Linux BIASBOAT, así como GOSSIPFLOW y LOADGRIP.

GOSSIPFLOW es un proxy SOCKS5 basado en Golang, mientras que LOADGRIP es un binario ELF escrito en C que se utiliza para cargar BIASBOAT en hosts Linux comprometidos.

Sandworm es un grupo de amenazas prolífico y altamente adaptable vinculado a la Unidad 74455 dentro de la Dirección Principal del Estado Mayor de las Fuerzas Armadas de la Federación Rusa (GRU). Se sabe que está activo desde al menos 2009, con el adversario también vinculado a tres personas activistas de hackeo y filtración, como XakNet Team, CyberArmyofRussia_Reborn y Solntsepek.

> *«Sponsorizado por la inteligencia militar rusa, APT44 es un actor de amenazas dinámico y operacionalmente maduro que está activamente comprometido en el espectro completo de espionaje, ataque y operaciones de influencia»,* dijo Mandiant, describiendo la amenaza persistente avanzada (APT) como comprometida en un esfuerzo de múltiples frentes para ayudar a Rusia a obtener una ventaja en tiempos de guerra desde enero de 2022.
>
> *«Las operaciones de APT44 tienen un alcance global y reflejan los amplios intereses y ambiciones nacionales de Rusia. Los patrones de actividad a lo largo del tiempo indican que APT44 tiene asignadas una serie de prioridades estratégicas diferentes y es muy probable que el Kremlin lo vea como un instrumento flexible de poder capaz de servir tanto a requisitos de inteligencia duraderos como emergentes».*