Actores respaldados por el gobierno ruso han ejecutado ataques de relevo de hash NT LAN Manager (NTLM) v2 a través de diversos métodos desde abril de 2022 hasta noviembre de 2023, dirigidos a objetivos de alto valor a nivel mundial.

Estos ataques, atribuidos a un grupo de piratas informáticos *«agresivos»* denominado APT28, se han focalizado en organizaciones vinculadas con asuntos internacionales, energía, defensa, transporte, así como en aquellas relacionadas con trabajo, bienestar social, finanzas, paternidad y gobiernos locales.

La firma de ciberseguridad Trend Micro ha evaluado estas intrusiones como un *«método eficiente para automatizar intentos de fuerza bruta»* en las redes de sus objetivos, destacando que el adversario podría haber comprometido miles de cuentas de correo electrónico con el tiempo.

APT28 es también conocido en la comunidad de ciberseguridad con otros nombres como Blue Athena, BlueDelta, Fancy Bear, Fighting Ursa, Forest Blizzard (anteriormente Strontium), FROZENLAKE, Iron Twilight, ITG05, Pawn Storm, Sednit, Sofacy y TA422.

Se cree que este grupo, activo desde al menos 2009, es operado por el servicio de inteligencia militar GRU de Rusia y tiene antecedentes de orquestar ataques de phishing que contienen archivos adjuntos maliciosos o compromisos estratégicos de sitios web para activar cadenas de infección.

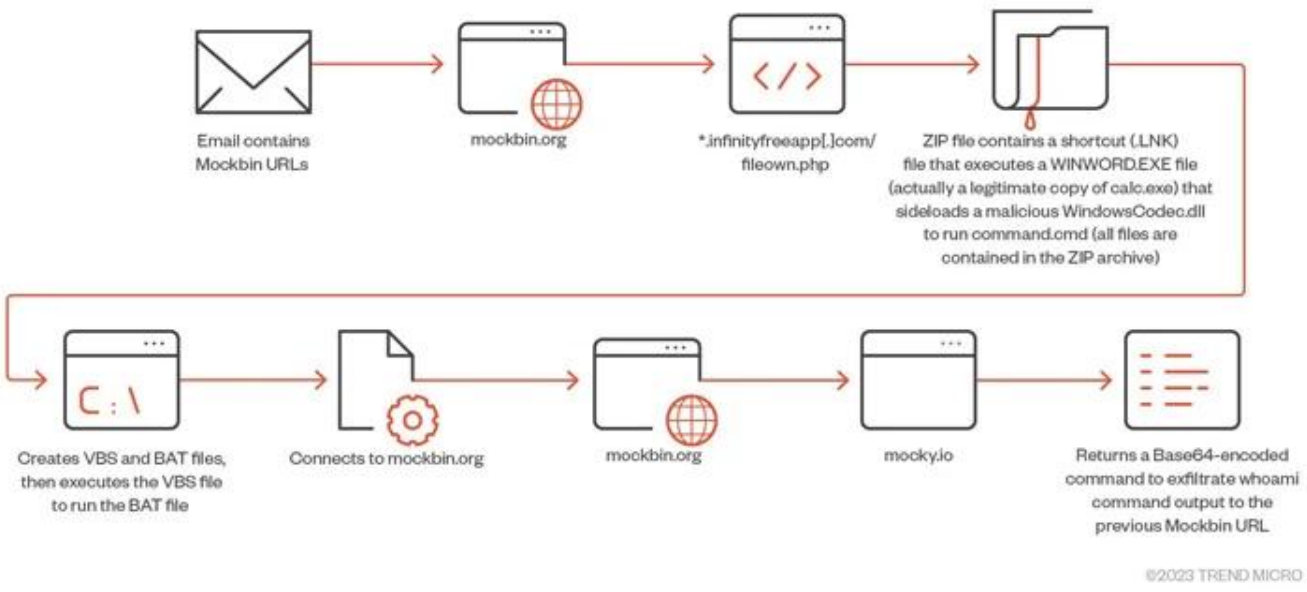
En abril de 2023, APT28 fue vinculado a ataques que aprovechaban vulnerabilidades ya parcheadas en equipos de red de Cisco para realizar reconocimiento y desplegar malware contra objetivos específicos.

Este actor estatal, en diciembre, fue objeto de atención por explotar una vulnerabilidad de escalada de privilegios en Microsoft Outlook (CVE-2023-23397, puntuación CVSS: 9.8) y WinRAR (CVE-2023-38831, puntuación CVSS: 7.8) para acceder al hash Net-NTLMv2 de un usuario y utilizarlo para llevar a cabo un ataque de relevo NTLM contra otro servicio para autenticarse como el usuario.

Se afirma que se utilizó un exploit para CVE-2023-23397 para atacar entidades ucranianas tan temprano como en abril de 2022, según un aviso de CERT-EU en marzo de 2023.

Además, se ha observado que utiliza señuelos relacionados con el conflicto entre Israel y Hamás para facilitar la entrega de una puerta trasera personalizada llamada HeadLace. También ha dirigido mensajes de phishing a entidades gubernamentales ucranianas y organizaciones polacas para desplegar puertas traseras y robar información utilizando herramientas como OCEANMAP, MASEPIE y STEELHOOK.

Un aspecto destacado de los ataques de este actor es su constante intento de mejorar sus tácticas operativas, ajustando y modificando enfoques para evadir la detección.



Esto incluye la incorporación de capas de anonimización como servicios VPN, Tor, direcciones IP de centros de datos y routers EdgeOS comprometidos para llevar a cabo actividades de escaneo y sondeo. Otra táctica consiste en enviar mensajes de phishing dirigidos desde cuentas de correo electrónico comprometidas a través de Tor o VPN.

> *«El grupo Pawn Storm también ha utilizado routers EdgeOS para enviar correos electrónicos de phishing, realizar llamadas de retorno de exploits de CVE-2023-23397 en Outlook y robar credenciales en sitios web de phishing de credenciales»,* señalaron los investigadores de seguridad Feike Hacquebord y Fernando Merces.

> *«Parte de las actividades posteriores a la explotación del grupo incluyen la modificación de permisos de carpetas dentro del buzón del correo de la víctima, lo que garantiza una persistencia mejorada. Utilizando las cuentas de correo electrónico de la víctima, es posible el movimiento lateral al enviar mensajes de correo electrónico maliciosos adicionales desde dentro de la organización de la víctima»,* agregaron los investigadores.

No se conoce actualmente si el actor en sí mismo comprometió estos routers o si está utilizando routers que ya fueron comprometidos por un actor de terceros. Sin embargo, se estima que al menos 100 routers EdgeOS han sido infectados.

Además, campañas recientes de recolección de credenciales contra gobiernos europeos han utilizado páginas de inicio de sesión falsas que imitan a Microsoft Outlook y se alojan en URLs de webhook[.]site, un patrón previamente atribuido al grupo.

No obstante, en una campaña de phishing en octubre de 2022, se dirigieron a embajadas y otras entidades de alto perfil para entregar un ladrón de información «simple» a través de correos electrónicos que capturaban archivos con extensiones específicas y los enviaban a un servicio gratuito de intercambio de archivos llamado Keep.sh.

> *«La estridencia de las campañas repetitivas, a menudo toscas y agresivas, ahoga la quietud, sutileza y complejidad de la intrusión inicial, así como las acciones posteriores a la explotación que podrían ocurrir una vez que Pawn Storm establece un punto de apoyo inicial en las organizaciones de las víctimas»,* comentaron los

> investigadores.

Este desarrollo coincide con la revelación de Recorded Future News sobre una campaña de hackeo en curso realizada por el actor ruso COLDRIVER (también conocido como Calisto, Iron Frontier o Star Blizzard), que se hace pasar por investigadores y académicos para redirigir a posibles víctimas a páginas de recolección de credenciales.