El grupo de hackers patrocinado por el Estado iraní conocido como MuddyWater (también identificado como Mango Sandstorm, Seedworm y Static Kitten) fue vinculado a un ataque de ransomware descrito como una operación de "falsa bandera".

El ataque, detectado por Rapid7 a comienzos de 2026, utilizó técnicas de ingeniería social a través de Microsoft Teams para iniciar la cadena de infección. Aunque inicialmente el incidente parecía relacionado con una operación de ransomware-as-a-service (RaaS) asociada a la marca Chaos, las evidencias apuntan a un ataque selectivo respaldado por un Estado que simulaba ser una campaña común de extorsión.

*"La campaña estuvo marcada por una fase de ingeniería social altamente interactiva realizada mediante Microsoft Teams, donde los atacantes aprovecharon sesiones de compartición de pantalla para robar credenciales y manipular mecanismos de autenticación multifactor (MFA)"*, indicó Rapid7 en un informe.

*"Una vez dentro del entorno, el grupo evitó los flujos tradicionales de ransomware y optó por la exfiltración de datos y la persistencia a largo plazo mediante herramientas de administración remota como DWAgent, en lugar de cifrar archivos"*, agregó la compañía.

Los hallazgos sugieren que MuddyWater intenta dificultar los esfuerzos de atribución utilizando herramientas comerciales y utilidades fácilmente disponibles en el ecosistema del cibercrimen. Este cambio de estrategia también ha sido documentado recientemente por Ctrl-Alt-Intel, Broadcom, Check Point y JUMPSEC, destacando el uso de herramientas como CastleRAT y Tsundere.

No obstante, esta no es la primera ocasión en la que MuddyWater participa en ataques de ransomware. En septiembre de 2020, el grupo fue relacionado con una campaña contra organizaciones israelíes de alto perfil mediante un loader llamado PowGoop, el cual desplegaba una variante destructiva del ransomware Thanos.

Posteriormente, en 2023, Microsoft reveló que el grupo colaboró con DEV-1084, un actor de amenazas asociado con la identidad DarkBit, para ejecutar ataques destructivos disfrazados

de operaciones ransomware. Más recientemente, en octubre de 2025, los atacantes habrían utilizado el ransomware Qilin para atacar un hospital gubernamental israelí.

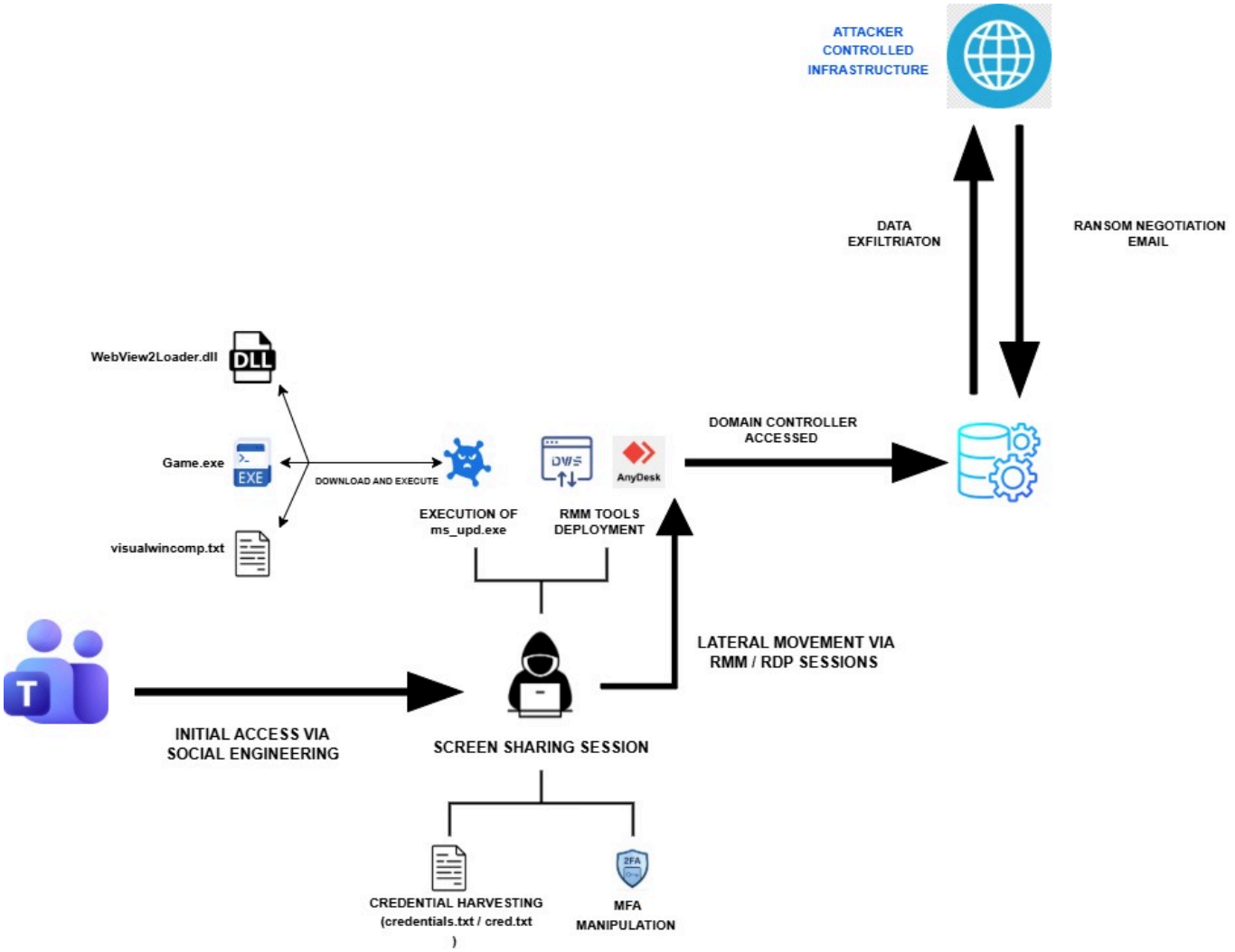
*"En este caso, el panorama emergente indicaba que los atacantes probablemente eran operadores vinculados a Irán que actuaban dentro del ecosistema criminal cibernético, utilizando una marca de ransomware criminal y métodos asociados al mercado general de extorsión, mientras perseguían objetivos estratégicos iraníes"*, señaló Check Point en marzo pasado.

*"El uso de Qilin y la participación en su programa de afiliados probablemente no solo proporciona una capa adicional de encubrimiento y negación plausible, sino que también actúa como un facilitador operativo importante, especialmente porque ataques anteriores parecen haber incrementado las medidas de seguridad y monitoreo por parte de las autoridades israelíes"*, añadió la firma.

Chaos es un grupo RaaS surgido a inicios de 2025. Conocido por aplicar un modelo de doble extorsión, el grupo promocionó su programa de afiliados en foros de ciberdelincuencia como RAMP y RehubCom.

Las operaciones de este grupo combinan campañas de saturación de correos electrónicos y vishing mediante Microsoft Teams, generalmente haciéndose pasar por personal de soporte técnico para convencer a las víctimas de instalar herramientas de acceso remoto como Microsoft Quick Assist. Posteriormente, aprovechan ese acceso inicial para profundizar en el entorno comprometido y desplegar ransomware.

*"El grupo también ha demostrado capacidades de triple extorsión al amenazar con ataques de denegación de servicio distribuido (DDoS) contra la infraestructura de las víctimas"*, explicó Rapid7.




*"Estas capacidades aparentemente forman parte de servicios integrados ofrecidos a afiliados, representando una característica relevante de su modelo RaaS. Además, Chaos también ha mostrado elementos de cuádruple extorsión, incluyendo amenazas de contactar clientes o competidores para aumentar la presión sobre las víctimas"*, añadió la empresa.

Hasta finales de marzo de 2026, Chaos aseguraba haber comprometido a 36 víctimas en su portal de filtraciones, principalmente en Estados Unidos. Los sectores más afectados incluyen construcción, manufactura y servicios empresariales.

En la intrusión analizada por Rapid7, el actor de amenazas inició solicitudes de chat externas mediante Teams para interactuar con empleados y obtener acceso inicial mediante sesiones de pantalla compartida. Posteriormente, utilizó cuentas comprometidas para realizar reconocimiento interno, establecer persistencia mediante herramientas como DWAgent y AnyDesk, desplazarse lateralmente y exfiltrar información. Finalmente, la víctima fue contactada por correo electrónico para iniciar negociaciones de rescate.

*"Mientras permanecía conectado, el actor ejecutó comandos básicos de reconocimiento, accedió a archivos relacionados con la configuración VPN de la víctima e instruyó a usuarios para ingresar sus credenciales en archivos de texto creados localmente"*, detalló Rapid7.

*"En al menos un caso, el actor también desplegó una herramienta de administración remota (AnyDesk) para facilitar aún más el acceso"*, añadió la compañía.

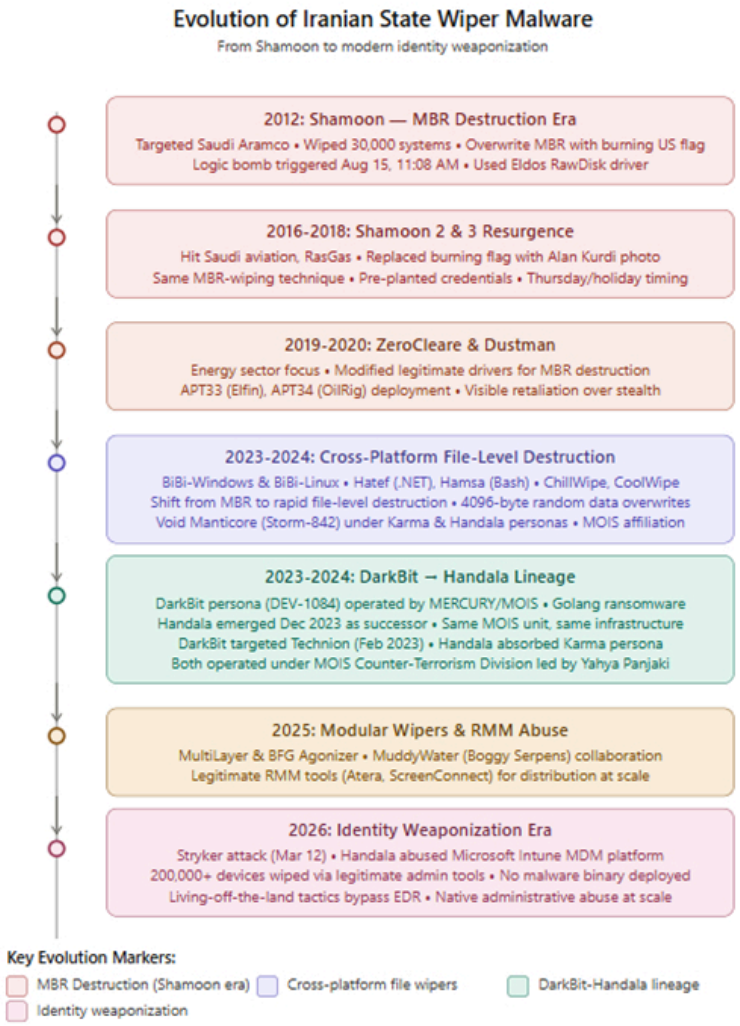
Los investigadores también observaron el uso de RDP para descargar un ejecutable denominado "ms_upd.exe" desde un servidor externo utilizando la utilidad curl. Tras ejecutarse, el archivo iniciaba una cadena de infección de múltiples etapas diseñada para desplegar componentes maliciosos adicionales.

Entre las familias de malware identificadas destacan:

- ms_upd.exe (Stagecomp): recopila información del sistema y se comunica con un servidor de comando y control (C2) para descargar componentes adicionales.
- game.exe (Darkcomp): un troyano de acceso remoto (RAT) diseñado para aparentar ser una aplicación legítima de Microsoft WebView2.
- WebView2Loader.dll: una DLL legítima requerida por Microsoft Edge WebView2.
- visualwincomp.txt: archivo de configuración cifrado utilizado por el RAT para obtener información del servidor C2.

El RAT mantiene comunicación constante con el servidor C2 mediante consultas cada 60 segundos, permitiendo ejecutar comandos, scripts PowerShell, operaciones sobre archivos y sesiones interactivas de cmd.exe o PowerShell.

La vinculación de esta campaña con MuddyWater se basa en el uso de un certificado de firma de código atribuido a “Donald Gay”, empleado para firmar “ms_upd.exe”. Dicho certificado ya había sido utilizado anteriormente por el grupo para firmar malware, incluyendo un downloader CastleLoader conocido como Fakeset.




Estos hallazgos reflejan una creciente convergencia entre operaciones de intrusión patrocinadas por Estados y tácticas típicas del cibercrimen con el objetivo de dificultar la atribución y retrasar las respuestas defensivas.

*"El uso de un marco RaaS en este contexto podría permitir que el actor difumine las diferencias entre actividades patrocinadas por Estados y delitos cibernéticos motivados financieramente, complicando así la atribución"*, afirmó Rapid7.

*"Además, la inclusión de elementos de extorsión y negociación podría enfocar los esfuerzos defensivos en el impacto inmediato, retrasando probablemente la identificación de mecanismos de persistencia subyacentes establecidos mediante herramientas de acceso remoto como DWAgent o AnyDesk"*, agregó la firma.

*"Cabe destacar que la aparente ausencia de cifrado de archivos, pese a la presencia de artefactos del ransomware Chaos, representa una desviación del comportamiento habitual de este tipo de amenazas. Esta inconsistencia podría indicar que el componente ransomware funcionó principalmente como un mecanismo de facilitación u ofuscación, más que como el objetivo principal de la intrusión"*, concluyó Rapid7.

En declaraciones compartidas con The Hacker News, Sergey Shykevich, gerente de grupo en Check Point Research, aseguró que el uso de herramientas de cibercrimen por parte de grupos iraníes, incluido MuddyWater, ha ido en aumento.

*"Este enfoque les brinda mucha más flexibilidad operativa y acceso a amplios conjuntos de herramientas sin necesidad de invertir en desarrollo interno"*, señaló Shykevich.

*"También dificulta considerablemente la atribución, agregando una nueva capa de complejidad para los defensores que intentan rastrear a estos actores"*, añadió.

El desarrollo de estas actividades coincide con hallazgos recientes de Hunt.io sobre una operación vinculada a Irán dirigida contra instituciones gubernamentales de Omán, orientada a exfiltrar más de 26.000 registros de usuarios del Ministerio de Justicia, datos judiciales, decisiones de comités y registros del sistema.

*"Un directorio abierto en 172.86.76[.]127, alojado en un VPS de RouterHosting en Emiratos Árabes Unidos, expuso una campaña activa de intrusión contra el gobierno omaní, con*

*herramientas, código C2, registros de sesión y datos exfiltrados visibles públicamente”*, explicó la empresa.

*“El principal objetivo fue el Ministerio de Justicia y Asuntos Legales (mjla.gov[.]om)”*, añadió.

El descubrimiento también coincide con la actividad sostenida de grupos hacktivistas alineados con Irán, como Handala Hack, que aseguró haber publicado información de cerca de 400 miembros de la Marina de Estados Unidos en el Golfo Pérsico y realizado un ataque contra el Puerto de Fujairah, en Emiratos Árabes Unidos, obteniendo acceso a sistemas internos y filtrando aproximadamente 11.000 documentos sensibles relacionados con facturas, registros de envío y documentación aduanera.

*“Hace un mes documentamos una amplia escalada en operaciones cibernéticas vinculadas con Irán: vigilancia mediante cámaras comprometidas, filtración de miles de documentos altamente sensibles del ex jefe del Estado Mayor Militar de Israel y un aumento medible en el volumen de ataques en la región. En ese momento advertimos que era probable una mayor escalada”*, declaró Shykevich.

*“El supuesto ataque contra el Puerto de Fujairah representa precisamente esa escalada, si se confirma. Lo que ha cambiado es la naturaleza de la amenaza: esto ya no se trata únicamente de recopilación de inteligencia o humillación pública. Los datos robados de infraestructura portuaria presuntamente fueron utilizados para facilitar objetivos de ataque con misiles”*, añadió.

*“Los dominios cibernético y cinético ahora están claramente conectados. Esta campaña no muestra señales de desaceleración. Históricamente, cada período de calma en el frente físico ha sido seguido por una intensificación de la actividad cibernética, y lo que observamos actualmente es la manifestación más grave de ese patrón hasta la fecha”*, concluyó.