El Departamento de Justicia de EE. UU. (DoJ) anunció el jueves la interrupción de la infraestructura en línea vinculada con DanaBot (también conocido como DanaTools) y reveló cargos contra 16 personas presuntamente involucradas en el desarrollo y distribución del malware, el cual, según indicó, estaba bajo el control de una organización cibercriminal con base en Rusia.

De acuerdo con el DoJ, el malware infectó más de 300,000 computadoras en todo el mundo, facilitó fraudes, ataques de ransomware y causó pérdidas superiores a los $50 millones de dólares. Dos de los acusados, Aleksandr Stepanov (alias JimmBee), de 39 años, y Artem Aleksandrovich Kalinkin (alias Onix), de 34, ambos oriundos de Novosibirsk, Rusia, se encuentran prófugos.

Stepanov enfrenta cargos por conspiración, fraude electrónico y bancario, robo de identidad agravado, acceso no autorizado a computadoras protegidas, alteración de sistemas informáticos, interceptación de comunicaciones y uso de comunicaciones interceptadas. Kalinkin ha sido acusado de conspirar para acceder sin autorización a computadoras con fines de obtención de datos y fraude, así como de afectar de forma no autorizada sistemas informáticos protegidos.

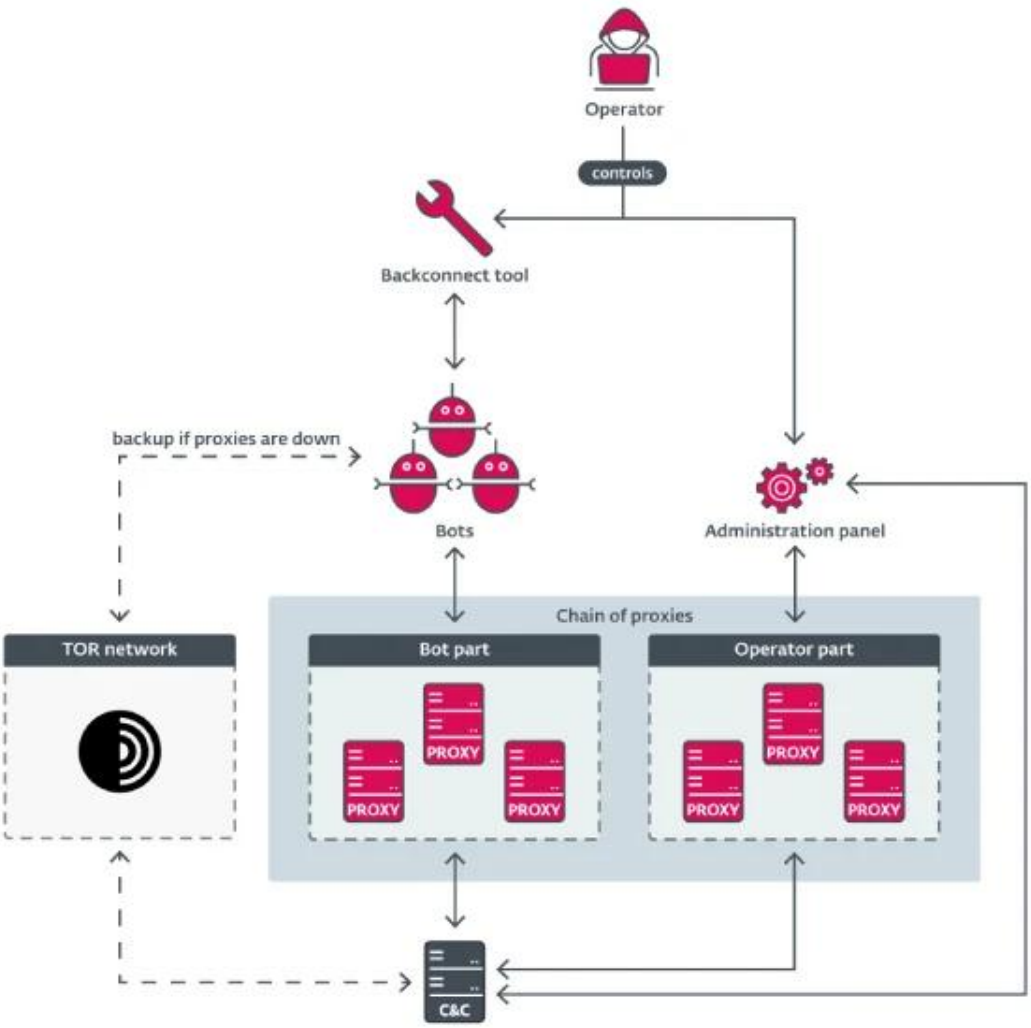
La denuncia penal y la acusación reveladas indican que varios de los acusados, incluido Kalinkin, habrían expuesto sus identidades reales tras infectar accidentalmente sus propios dispositivos con el malware.

> *"En algunos casos, tales auto-infecciones parecían intencionales, con el fin de probar, analizar o mejorar el malware. En otros, las infecciones fueron accidentales – uno de los riesgos del crimen cibernético es que los propios actores pueden infectarse con su propio software malicioso por error»*, señala la denuncia [PDF].
>
> *"Estas infecciones accidentales a menudo derivaron en la extracción de datos sensibles desde las computadoras de los propios delincuentes, los cuales fueron almacenados en los servidores de DanaBot, incluyendo información que permitió*

> *identificar a miembros de la organización criminal",* añade el documento.

Si Kalinkin resulta culpable, podría enfrentar una pena máxima de 72 años en prisión federal. Stepanov, por su parte, enfrentaría hasta cinco años de cárcel. En paralelo, la operación policial —como parte de la Operation Endgame— logró incautar los servidores de comando y control (C2) de DanaBot, incluidos decenas de servidores virtuales alojados en EE. UU.

> *"El malware DanaBot utilizaba múltiples métodos para infectar computadoras, incluyendo correos electrónicos de spam con archivos adjuntos maliciosos o enlaces peligrosos. Los dispositivos comprometidos pasaban a formar parte de una botnet, permitiendo a los operadores controlar de manera remota las computadoras afectadas"*, explicó el DoJ.



Al igual que Lumma Stealer, recientemente desmantelado, DanaBot funcionaba bajo un modelo de «malware como servicio» (MaaS), ofreciendo acceso al software desde $500 hasta varios miles de dólares al mes. Rastreado bajo los alias Scully Spider y Storm-1044, DanaBot es una herramienta versátil similar a Emotet, TrickBot, QakBot o IcedID, con capacidad para robar información y servir como plataforma de entrega de cargas maliciosas, como ransomware.

Este malware modular, escrito en Delphi, está diseñado para robar datos, secuestrar sesiones

bancarias, extraer credenciales, historiales de navegación y billeteras de criptomonedas. También puede brindar acceso remoto completo, registrar pulsaciones de teclado y grabar videos. DanaBot circula desde mayo de 2018, cuando apareció como un troyano bancario.

> *"DanaBot inicialmente apuntó a usuarios en Ucrania, Polonia, Italia, Alemania, Austria y Australia, antes de expandirse a instituciones financieras de EE. UU. y Canadá en octubre de 2018. Su popularidad creció debido al enfoque modular temprano, con soporte para inyecciones web tipo Zeus, funcionalidades de robo de información, grabación de pantalla y HVNC encubierto"*, indicó CrowdStrike.

Según Black Lotus Labs y Team Cymru, DanaBot emplea una arquitectura de comunicaciones en capas entre el dispositivo víctima y los controladores del botnet, en la cual el tráfico de C2 es redirigido a través de dos o tres niveles de servidores antes de alcanzar el destino. Se estima que siempre había entre cinco y seis servidores de segundo nivel activos. La mayoría de las víctimas se encuentran en Brasil, México y Estados Unidos.

> *"Los operadores han demostrado compromiso con su actividad, adaptándose a las detecciones y cambiando sus tácticas de defensa. En versiones posteriores, ocultaron mejor los C2 usando capas, dificultando su rastreo. También han hecho el bot más accesible mediante precios estructurados y soporte al cliente"*, explicaron ambas firmas.

Datos de Proofpoint muestran que DanaBot estuvo "casi completamente ausente" del panorama de amenazas por correo entre julio de 2020 y junio de 2024, lo cual indica que su propagación se realizó mediante otros métodos, como campañas de SEO malicioso y publicidad engañosa (malvertising).

El DoJ afirmó que los administradores de DanaBot operaban una segunda variante del botnet diseñada para atacar a organismos militares, diplomáticos y gubernamentales en

Norteamérica y Europa. Esta versión, aparecida en enero de 2021, tenía funciones para registrar toda la actividad en un equipo comprometido y enviar la información a un servidor distinto.

> *"Malware tan persistente como DanaBot perjudica a cientos de miles de víctimas en todo el mundo, incluyendo entidades sensibles, y genera pérdidas millonarias",* expresó el fiscal Bill Essayli del Distrito Central de California.

El DoJ también agradeció el apoyo de varias compañías del sector privado, incluyendo Amazon, CrowdStrike, ESET, Flashpoint, Google, Intel 471, Lumen, PayPal, Proofpoint, Spycloud, Team Cymru y Zscaler, por su "valiosa colaboración".

Aspectos clave de DanaBot según múltiples informes:

- El sub-botnet 5 fue usado para lanzar ataques DDoS contra sitios del Ministerio de Defensa y el Consejo de Seguridad Nacional de Ucrania en marzo de 2022.
- Los sub-botnets 24 y 25 estuvieron orientados a espionaje para intereses del gobierno ruso.
- Desde 2022, el grupo detrás del malware reestructuró su oferta para enfocarse en evadir defensas, con al menos 85 versiones diferentes identificadas hasta marzo de 2025 (la más reciente es la versión 4006).
- La infraestructura de DanaBot incluye varios componentes: el «bot», el «OnlineServer», el «cliente» y el «servidor».
- Se ha usado para espiar a funcionarios gubernamentales en Medio Oriente y Europa del Este.
- Los desarrolladores ofrecen el malware en alquiler a afiliados que crean sus propias redes de bots.
- Han colaborado con desarrolladores de otros cryptors y loaders como Matanbuchus.
- Mantenía un promedio diario de 150 servidores C2 de primer nivel y cerca de 1,000 víctimas diarias en más de 40 países, consolidándose como una de las plataformas MaaS más grandes en 2025.

> *"Las operaciones contra cibercriminales como DanaBot afectan la operatividad de los malware y generan costos a los delincuentes al forzarlos a cambiar tácticas y a desconfiar entre ellos. El éxito de estas acciones depende de la cooperación entre el sector público y privado"*, dijo Selena Larson, investigadora de Proofpoint.

Cargos contra líder de QakBot

En paralelo, el DoJ también presentó cargos contra Rustam Rafailevich Gallyamov, de 48 años y residente en Moscú, acusado de liderar el desarrollo y operación de QakBot, otro malware desmantelado en una operación internacional en agosto de 2023. Además, se presentó una demanda de confiscación civil por más de $24 millones en criptomonedas incautadas durante la investigación.

> *"Gallyamov desarrolló, desplegó y controló el malware Qakbot desde 2008", señaló el DoJ. "Desde 2019, usó Qakbot para infectar miles de computadoras y crear una botnet global".*

Tras su caída, Gallyamov y sus cómplices continuaron con sus actividades delictivas mediante tácticas como ataques de spam masivo para infiltrarse en redes y desplegar ransomware como Black Basta y CACTUS, incluso hasta enero de 2025.

> *"Aunque su red fue neutralizada en 2023, Gallyamov siguió activamente propagando malware y colaborando con grupos criminales cibernéticos"*, declaró Akil Davis, del FBI en Los Ángeles.