El gobierno ruso advirtió este jueves sobre ataques cibernéticos dirigidos a operadores de infraestructura crítica nacionales, cuando la invasión total de Ucrania por parte del país ya entró en el segundo día.

Además de advertir sobre *«la amenaza de un aumento en la intensidad de los ataques informáticos»*, el Centro Nacional de Coordinación y Respuesta a Incidentes Informáticos de Rusia, dijo que *«los ataques pueden tener como objetivo interrumpir el funcionamiento de importantes recursos y servicios de información, causando daños a la reputación, incluso con fines políticos».*

> *«Cualquier falla en la operación de los objetivos debido a una razón que no se ha establecido de forma confiable, en primer lugar, debe considerarse como resultado de un ataque informático»,* dijo la agencia.

Además, notificó sobre posibles operaciones de influencia realizadas para *«formar una imagen negativa de la Federación Rusa a los ojos de la comunidad mundial»,* esto al hacerse eco de una alerta similar publicada por la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) la semana pasada, sobre esfuerzos de manipulación de información de actores extranjeros para golpear entidades críticas.

Sin embargo, la agencia no compartió más detalles acerca de la naturaleza de los ataques o su procedencia.

El aviso se produce cuando varios sitios web gubernamentales y bancarios en Rusia, incluido el militar (mil.ru), el Kremlin (kremlin.ru) y la Duma estatal (duma.gov.ru), se volvieron inaccesibles en medio de una avalancha de ataques cibernéticos ofensivos dirigidos a Ucrania, que resultaron en el despliegue de un limpiador de datos llamado HermeticWiper en cientos de máquinas en la nación de Europa del Este.

> *«Es importante tener en cuenta que el limpiador aprovecha los altos privilegios en*

> *el host comprometido para hacer que el host sea 'no arrancable' anulando los registros y configuraciones de arranque, borrando configuraciones de dispositivos y eliminando instantáneas»,* dijo Lavi Lazarovits, jefe de investigación de seguridad en CyberArk Labs.

> *«El limpiador está configurado para no encriptar los controladores de dominio, es decir, para mantener el dominio en funcionamiento y permitir que el ransomware use credenciales válidas para autenticarse en los servidores y encriptarlos. Esto destaca aún más que los actores de amenazas usan identidades comprometidas para acceder a la red y/o moverse lateralmente»,* dijo Lazarovitz.

No está claro cuántas redes se han visto afectadas por el malware de borrado de datos nunca antes visto, que se dirigió a organizaciones en las industrias financiera, de defensa, aviación y TI, según Symantec. La empresa propiedad de Broadcom también dijo que observó evidencia de ataques de limpiaparabrisas contra máquinas en Lituania, lo que implica un efecto indirecto.

Además, las acciones de HermeticWiper se superponen con otro limpiador de datos llamado WhisperGate que se informó por primera vez como utilizado contra organizaciones ucranianas en enero. Al igual que este último, el malware recién descubierto va acompañado de la distribución de una variedad de ransomware en los sistemas comprometidos.

El ransomware es un archivo .exe de 64 bits y 3.14 MB, escrito en Golang, según el ingeniero de respuesta a incidentes de Cybereason, Chen Erlich, quién compartió un análisis preliminar del ejecutable.

> *«Parece probable que el ransomware se haya utilizado como señuelo o distracción de los ataques del limpiaparabrisas. Esto tiene algunas similitudes con los anteriores ataques de Whispergate con el limpiaparabrisas contra Ucrania, donde el*

> *limpiaparabrisas estaba disfrazado de ransomware»,* dijo Symantec.

El análisis forense inicial sugiere que los ataques pueden haber estado en modo de preparación durante al menos tres meses, con actividad maliciosa potencialmente relacionada detectada en una organización lituana el 12 de noviembre de 2021. Además, se descubrió que una de las muestras de HermeticWiper tenía una marca de tiempo de compilación del 28 de diciembre de 2021.

Aunque las últimas acciones disruptivas aún no se atribuyen formalmente, los gobiernos del Reino Unido y Estados Unidos vincularon los ataques DDoS en Ucrania a mediados de febrero con la Dirección Principal de Inteligencia de Rusia (también conocida como GRU).

A medida que los ataques siguen desarrollándose tanto en el ámbito físico como el digital, Reuters informó que el gobierno ucraniano está buscando la ayuda de la comunidad clandestina de piratas informáticos en el país para defenderse de las infiltraciones cibernéticas dirigidas a la infraestructura crítica y realizar misiones de espionaje encubiertas contra los invasores rusos.