TLP:CLEAR

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

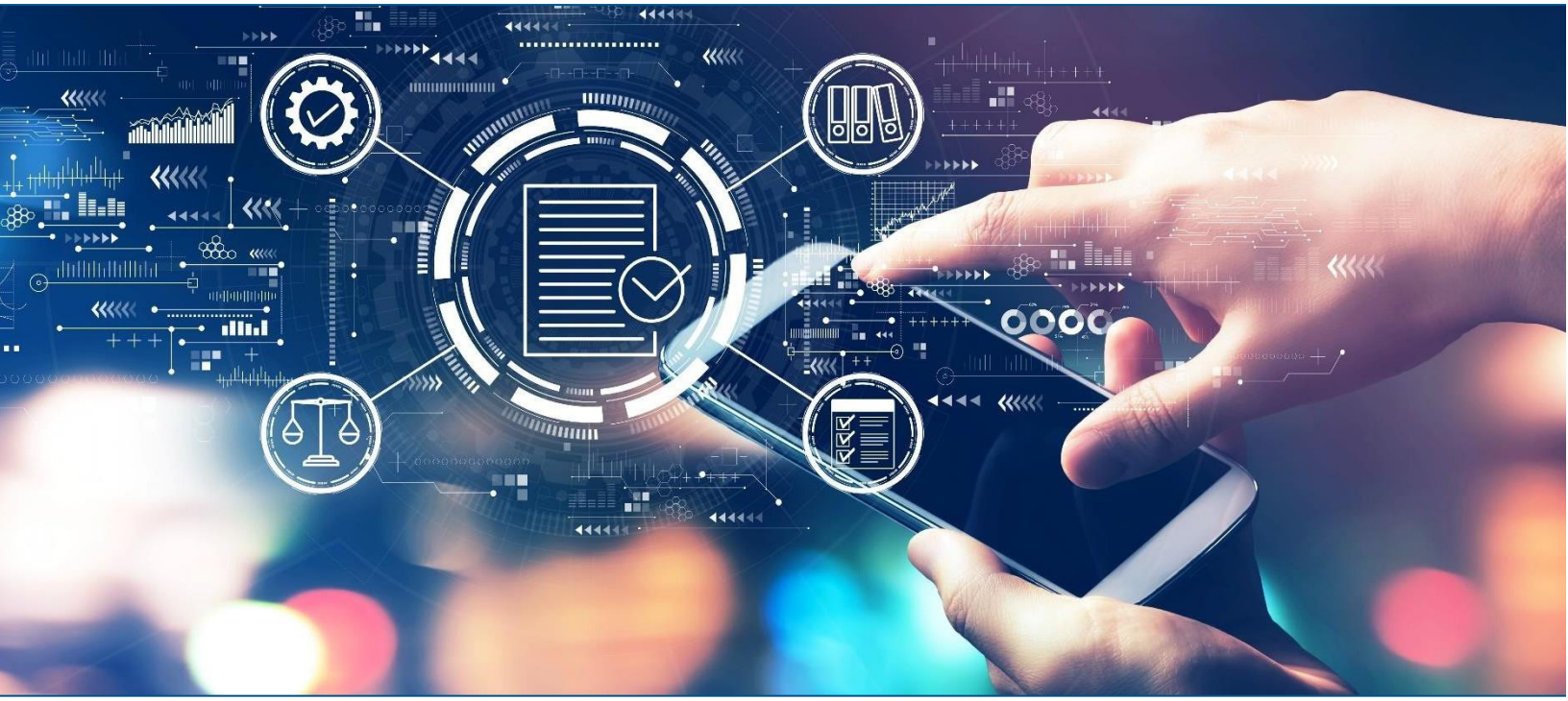
JPCERT CC®

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

警察庁
National Police Agency

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

National Cyber Security Centre
a part of GCHQ



Mitigación de las amenazas cibernéticas con recursos limitados: guía para la sociedad civil

Publicación: 14 de mayo de 2024

TLP:CLEAR

Resumen ejecutivo

La Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) de los Estados Unidos y las siguientes organizaciones (en adelante, las "agencias autoras") redactaron y fueron coautores de esta guía, en coordinación con importantes socios gubernamentales, no gubernamentales, industriales y de la sociedad civil. Las agencias autoras publican esta guía conjunta para brindar orientación sobre ciberseguridad a entidades comunitarias de alto riesgo (HRC, por sus siglas en inglés), como organizaciones y personas de la sociedad civil:

- Oficina de Inteligencia y Análisis del Departamento de Seguridad Nacional (DHS I&A, por sus siglas en inglés)
- Oficina Federal de Investigaciones (FBI, por sus siglas en inglés)
- Centro Canadiense de Ciberseguridad (CCCS, por sus siglas en inglés) (Centro Cibernético)
- Centro Nacional de Ciberseguridad de Estonia (NCSC-EE, por sus siglas en inglés)
- Centro de Coordinación del Equipo de Respuesta a Emergencias Informáticas de Japón (JPCERT/CC, por sus siglas en inglés)
- Centro Nacional de Preparación para Incidentes y Estrategia de Ciberseguridad (NISC, por sus siglas en inglés) de Japón
- Centro Nacional de Ciberseguridad de Finlandia (NCSC-FI, por sus siglas en inglés)
- Agencia de la Policía Nacional (NPA, por sus siglas en inglés) de Japón
- Centro Nacional de Ciberseguridad del Reino Unido (NCSC-UK, por sus siglas en inglés)

La sociedad civil, es decir, organizaciones y comunidades sin ánimo de lucro, culturales, religiosas, académicas, de investigación, de periodistas, de disidentes y de la diáspora implicadas en la defensa de los derechos humanos y el avance de la democracia, se consideran comunidades de alto riesgo. A menudo, estas organizaciones y sus empleados son blanco de amenazas estatales que pretenden socavar los valores e intereses democráticos. Este tipo de represión transnacional (también denominada represión transnacional digital), que se lleva a cabo con regularidad, consiste en que agentes patrocinados por el Estado ponen en peligro dispositivos y redes personales o de organizaciones para intimidar, silenciar, coaccionar, acosar o perjudicar a organizaciones y personas de la sociedad civil.

Según los informes de la industria, los ataques patrocinados por el Estado contra comunidades de alto riesgo proceden principalmente de los Gobiernos de Rusia, China, Irán y Corea del Norte. Los agentes suelen realizar investigaciones preoperativas exhaustivas para conocer a las posibles víctimas, recopilar información para respaldar la ingeniería social u obtener credenciales de inicio de sesión. Los agentes atacan las redes de las organizaciones o las cuentas personales (por ejemplo, de correo electrónico), así como los dispositivos de las personas para vigilarlos y controlarlos, a menudo mediante aplicaciones espía, es decir, software malicioso que recopila datos de los dispositivos afectados.

Esta guía proporciona recomendaciones para que organizaciones y personas de la sociedad civil mitiguen la amenaza de operaciones cibernéticas patrocinadas por el Estado basándose en el comportamiento malicioso observado. La guía también proporciona recomendaciones para que los fabricantes de software mejoren la postura de seguridad de sus clientes.

Índice

Introducción

Los informes de la industria enfatizan la prevalencia y la naturaleza global de las amenazas cibernéticas a la sociedad civil, lo que requiere su preparación contra una gama diversa de agentes de amenazas con motivaciones políticas e ideológicas. Las organizaciones de la sociedad civil se consideran comunidades de alto riesgo (HRC) debido a su alto nivel de amenaza y baja capacidad de defensa. En concreto:

- Las organizaciones de la sociedad civil y su personal corren ***un gran riesgo*** de ser el blanco de ciberagentes malintencionados. Según los informes de la industria, estas organizaciones y su personal son objetivos conocidos, ya que los agentes estatales pueden intentar socavar los valores democráticos.
- Las organizaciones de la sociedad civil suelen tener una ***baja capacidad de defensa***. Estas organizaciones carecen de soporte informático interno y de higiene cibernética esencial para evitar la posibilidad de actividad maliciosa (por ejemplo, gestión del ciclo de vida, gestión de parches, autenticación multifactor, gestión de contraseñas). Las personas que forman parte de la sociedad civil a menudo dependen de canales de comunicación inseguros y necesitan gestionar perfiles públicos para impulsar su labor. Las organizaciones con baja capacidad de defensa están mal preparadas y son vulnerables a las ciberamenazas comunes, como los intentos de ingeniería social.

La baja capacidad de defensa se ve agravada, en la mayoría de los casos, por productos y servicios diseñados de forma que la carga de reducir las ciberamenazas recae en el cliente o usuario final. Por ejemplo, se requiere que el cliente o usuario final tome medidas específicas, a veces onerosas, para mejorar su postura cibernética.

Esta guía conjunta, desarrollada como parte de la iniciativa de protección comunitaria de alto riesgo (HRCP, por sus siglas en inglés) de la CISA* y la campaña de defensa de la democracia del NCSC-UK†, proporciona medidas de mitigación para que las organizaciones de la sociedad civil reduzcan su riesgo en función de amenazas cibernéticas comunes. Las agencias autoras animan encarecidamente a las organizaciones de la sociedad civil y a las personas afiliadas a que apliquen las medidas de mitigación previstas en esta guía conjunta. Dichas agencias también animan a los fabricantes de software a asumir la responsabilidad de los resultados de seguridad de sus clientes

* Establecida en 2023, la iniciativa de HRCP de la CISA es la sede permanente del trabajo de dicha agencia para identificar y colaborar con las comunidades de alto riesgo con el fin de comprender las amenazas a las que se enfrentan, identificar los recursos que pueden reforzar su defensa y eliminar las deficiencias en el apoyo. Para obtener información sobre dicha iniciativa, consulte el comunicado de prensa del Departamento de Seguridad Nacional El secretario Mayorkas analiza los nuevos esfuerzos de Estados Unidos para contrarrestar la propagación del autoritarismo digital en la Cumbre para la Democracia.

† El Centro Nacional de Ciberseguridad del Reino Unido (NCSC-UK) adopta un enfoque integral de la ciberdefensa y considera a la sociedad civil como uno de los tres sectores en los que se centra su trabajo. A través de su trabajo de defensa de la democracia, dicho centro busca asociarse con funcionarios públicos y electos de alto riesgo para avanzar en la comprensión de las amenazas sofisticadas que atacan a las personas en dispositivos personales y empresariales. Para obtener más información, consulte la página web del Centro Nacional de Ciberseguridad del Reino Unido (NCSC-UK) Defensa de la democracia.

mediante la aplicación de las mitigaciones contenidas en este aviso y el diseño de productos que prevengan las clases más comunes de ataques por parte de agentes malintencionados.‡

Amenazas cibernéticas a la sociedad civil

La falta de información en la telemetría de amenazas y los flujos de inteligencia, junto con la accesibilidad limitada de las HRC a soluciones de nivel empresarial, dificulta a las organizaciones comerciales y gubernamentales la medición precisa de las amenazas que reciben dichas comunidades. Sin embargo, los informes de la industria indican un patrón consistente de agentes cibernéticos patrocinados por el Estado que apuntan a segmentos específicos de la sociedad civil. En particular, y con frecuencia, las organizaciones no gubernamentales (NGO, por sus siglas en inglés), los grupos de expertos, los activistas de derechos humanos y los periodistas son el objetivo de agentes patrocinados por el Estado:

- Según Microsoft, en 2023, las NGO y los grupos de expertos fueron los segundos objetivos más importantes de los agentes patrocinados por el Estado (después del sector de tecnología de la información).[1]
- En noviembre de 2023, un informe de CrowdStrike reveló que se sabe que cinco grupos patrocinados por el Estado atacan a grupos de expertos,[2] once grupos representan amenazas potenciales para las NGO,[3] dos grupos atacan a los disidentes[4] y uno ataca a organizaciones sin fines de lucro (NPO, por sus siglas en inglés).[5]
- Cloudflare ha observado que la actividad cibernética maliciosa contra organizaciones de la sociedad civil está "aumentando en general".[6] En el segundo trimestre de 2023, las NPO fueron el blanco de los ataques en mayor medida que cualquier otro sector cuando se analiza el tráfico malicioso a sitios web de dichas organizaciones como proporción del tráfico total.[7] En el tercer trimestre de 2023, las NPO y las organizaciones de medios independientes ocuparon el segundo lugar detrás de la industria de los metales y la minería, con un 17.14 % de todo el tráfico dirigido a las primeras que representa ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés).[8] De manera similar, la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés) descubrió que las personas de la sociedad civil eran el segundo sector más atacado en todo el mundo entre julio de 2022 y junio de 2023.[9]

Los agentes patrocinados por el Estado atacan a las organizaciones de la sociedad civil y a su personal como parte de su conjunto de herramientas para socavar los valores democráticos. En concreto, apuntan a organizaciones y personas en línea principalmente como un medio de intimidación, acoso,§ coerción y vigilancia; un tipo de represión transnacional llamada represión transnacional digital.

---

‡ Los productos diseñados pensando en la seguridad y la protección se denominan "seguros desde el diseño". Un principio clave de la seguridad desde el diseño es que los fabricantes de software se responsabilicen de los resultados de seguridad de sus clientes incorporando la ciberseguridad en el diseño y el desarrollo. Para obtener más información sobre la seguridad desde el diseño, consulte cisa.gov/securebydesign y la guía conjunta Cambio del equilibrio de los riesgos de ciberseguridad: principios y enfoques para la seguridad desde el diseño y por defecto.

§ El acoso, como herramienta independiente, lo utilizan los Estados para silenciar, controlar o reprimir a los disidentes, y el acoso digital es cuando se produce en línea, por ejemplo, mediante la movilización de cuentas de redes sociales contra personas.

La represión transnacional digital suele ir precedida de una extensa investigación en línea de sitios web corporativos, páginas de redes sociales, publicaciones geopolíticas y comunicados de prensa para que los agentes puedan recopilar información sobre las organizaciones y personas objetivo. Después de la investigación, los agentes patrocinados por el Estado a menudo obtienen acceso a redes de organizaciones o dispositivos personales a través de (a) ingeniería social que incita a las víctimas a divulgar las credenciales de sus cuentas o descargar programas maliciosos, o (b) hacer que los usuarios descarguen aplicaciones aparentemente legítimas que albergan software malicioso. Después de obtener acceso a los dispositivos, los agentes suelen instalar programas espía en ellos. Los programas espía son una herramienta comercial que proporciona amplias capacidades de vigilancia, incluido el seguimiento de la ubicación, la captura de imágenes y audio, así como el acceso a archivos y comunicaciones personales.

Para obtener más información sobre los grupos patrocinados por el Estado que se sabe que atacan a las organizaciones de la sociedad civil, consulte el Apéndice A: Agentes patrocinados por el Estado. Para obtener información técnica sobre las operaciones cibernéticas que permiten a los agentes obtener acceso a redes y dispositivos, y vigilar y monitorear a las personas, consulte el Apéndice B: Tácticas y técnicas de los agentes patrocinados por el Estado.

Medidas de mitigación

Organizaciones de la sociedad civil

CARACTERÍSTICAS CLAVE DE LOS CPG:

- Subconjunto priorizado de prácticas de ciberseguridad.
- Prioritarios para la reducción de riesgos.
- Se basan en las amenazas observadas por la CISA y sus socios gubernamentales e industriales.
- Pretenden reducir significativamente los riesgos tanto para las operaciones de infraestructuras críticas como para el público.

Las agencias autoras animan firmemente a las organizaciones de la sociedad civil a implementar las prácticas recomendadas según lo definido por los objetivos de desempeño en ciberseguridad (CPG, por sus siglas en inglés) intersectoriales de la CISA. Estos controles de ciberseguridad proporcionan un conjunto mínimo de prácticas y protecciones que se basan en las amenazas y los comportamientos más comunes e impactantes. Para mitigar la posibilidad de que agentes patrocinados por el Estado lleven a cabo actividades de reconocimiento y obtengan acceso inicial a las redes de la empresa mediante la suplantación de identidad y el compromiso de credenciales, dé prioridad a lo siguiente:

1) **Mantenga el software actualizado en los dispositivos de los usuarios y en la infraestructura informática.** Las actualizaciones de software corrigen fallas conocidas. Instalarlas lo antes posible significa que los agentes no pueden aprovechar estas fallas para acceder a los sistemas.
2) **Implemente una autenticación multifactor (MFA, por sus siglas en inglés) resistente a la suplantación de identidad** [CPG 2.H]. La configuración de MFA resistente a la suplantación de identidad hace que sea más difícil para los agentes comprometer las cuentas de los usuarios y, a menudo, simplifica al mismo tiempo los inicios de sesión legítimos de los usuarios. Consulte la guía de autenticación multifactor resistente a la suplantación de identidad de la CISA para obtener información adicional.
3) **Audite las cuentas y desactive las que no utilice o sean innecesarias.** Elimine las cuentas innecesarias para reducir los vectores de acceso que los agentes pueden utilizar para ingresar al sistema.
4) **Deshabilite las cuentas de usuario y el acceso a los recursos de la organización para el personal saliente** [CPG 2.D]. La desactivación de cuentas puede minimizar la exposición del sistema, ya que elimina las opciones que los agentes pueden aprovechar para entrar en el sistema.
5) **Aplique el principio del privilegio mínimo.** Audite las cuentas con permisos amplios o de alto impacto (acceso de administrador) y elimine cualquier permiso innecesario para reducir el daño que los agentes pueden infligir mediante una cuenta comprometida. Evite usar cuentas de usuarios administradores para tareas diarias habituales [CPG 2.E]. El uso de las cuentas de usuarios administradores debe monitorearse periódicamente a fin de detectar actividades maliciosas y no autorizadas.
6) **Ejerza la diligencia debida al seleccionar proveedores, incluidos los proveedores de servicios en la nube (CSP, por sus siglas en inglés) y los proveedores de servicios administrados (MSP, por sus siglas en inglés).** Esto reduce los riesgos de la cadena de suministro. Utilice únicamente proveedores acreditados que expresen verbalmente cómo adoptan las prácticas

de seguridad desde el diseño. Consulte la sección "Fabricantes de software" para conocer el compromiso de seguridad desde el diseño de la CISA y las prácticas recomendadas.

7) **Revise las relaciones contractuales** con todos los proveedores de servicios y dé prioridad a los proveedores de servicios críticos. Asegúrese de que los contratos incluyan lo siguiente:
   - Controles de seguridad diseñados para satisfacer las necesidades específicas de los clientes.
   - Supervisión y registro apropiados de los sistemas de clientes administrados por el proveedor.
   - Supervisión continua de la presencia, las actividades y las conexiones del proveedor de servicios a la red del cliente, garantizando el cumplimiento de los objetivos de rendimiento de ciberseguridad y los principios de seguridad desde el diseño.
   - Notificación a un destinatario actualizado de los sucesos e incidentes de seguridad confirmados o sospechosos que se produzcan en la infraestructura y la red administrativa del proveedor.
8) **Gestione los riesgos de la arquitectura** mediante lo siguiente:
   - Auditoría y revisión de las conexiones entre los sistemas de los clientes, los sistemas de los proveedores de servicios y otros enclaves de los clientes; en particular, los expuestos a Internet, como los servicios en la nube, los servidores de correo electrónico y los servidores de redes privadas virtuales (VPN, por sus siglas en inglés).
   - Uso de una red privada virtual (VPN) dedicada para conectarse a la infraestructura del proveedor de servicios administrados (MSP); todo el tráfico de red procedente de dicho proveedor solo debe atravesar esta conexión segura dedicada.
9) **Implemente una capacitación básica en ciberseguridad** para cubrir conceptos como suplantación de identidad de cuentas, seguridad de navegación web y correo electrónico, y seguridad de contraseñas [CPG 2.I]. Asegúrese de que la capacitación aborde los ataques de ciberagentes patrocinados por el Estado contra correos electrónicos y dispositivos personales, y de que el personal proteja sus cuentas de correo electrónico y dispositivos móviles personales de cualquier peligro, mediante la aplicación de las recomendaciones que figuran a continuación.
10) **Desarrolle y ponga en práctica planes de respuesta a incidentes y de recuperación** [CPG 2.S]. Asegúrese de que los planes cubran al menos los sistemas que son críticos e importantes para la organización e incluyan a quién contactar o a quién informar del incidente para obtener ayuda. Consulte la sección "Información de contacto" de esta guía para obtener información de la agencia autora correspondiente. Consulte la sección "Recursos" para obtener orientación sobre cómo crear planes de recuperación y respuesta a incidentes.

Personas de la sociedad civil

Las agencias autoras instan encarecidamente a las personas de la sociedad civil a poner en práctica las siguientes recomendaciones para mitigar el impacto de los agentes patrocinados por el Estado que obtienen acceso a las redes corporativas, así como a los dispositivos móviles, con fines de vigilancia y control. Estas mitigaciones se alinean con el Proyecto Upskill de la CISA. Dicho proyecto, desarrollado como parte del esfuerzo de planificación de protección de comunidades de alto riesgo de 2023 de la Colaboración Conjunta de Defensa Cibernética (JCDC, por sus siglas en inglés) de la agencia, es una serie de guías para ayudar a los usuarios no técnicos a mejorar su seguridad digital. Consulte el Proyecto Upskill para obtener detalles y orientación sobre cómo implementar las siguientes recomendaciones.

- **Utilice contraseñas seguras en las cuentas e implemente la MFA** [Proyecto Upskill, módulo 2, tema 2.0, tema 2.2].
  - **Utilice soluciones sólidas de MFA,** como tokens digitales o de equipos, para proteger las cuentas.
- **Limite la exposición de la información disponible públicamente.**
  - **Sea prudente en las redes sociales** y en línea. Tenga cuidado con la información que introduce en las plataformas públicas.
  - **Promueva la limitación de los datos compartidos entre amigos y familiares**, lo que aumenta la seguridad general frente a posibles explotaciones.
- **Verifique los contactos y esté atento a la ingeniería social**. Para mejorar la ciberseguridad personal y de la organización, es esencial comprender las amenazas y los comportamientos específicos relevantes para su industria o para sí mismo. Establezca una lista de referencia que describa las amenazas potenciales y tenga en cuenta el singular panorama de riesgos asociado a su trabajo, intereses y organizaciones. Esto puede incluir amenazas cibernéticas específicas de la industria, consideraciones regulatorias y patrones de ataque históricos.
  - **Confirme las identidades de los contactos de las redes sociales** a fin de mitigar el riesgo de perfiles falsos y tácticas de ingeniería social.
  - **Manténgase atento a los intentos de suplantación de identidad**, sobre todo de personas que dicen ser periodistas u otros perfiles.
  - **Sea prudente al hacer clic en los enlaces o archivos adjuntos** en correos electrónicos, mensajes de texto u otras plataformas de comunicación.
  - **Sea prudente al hacer clic en enlaces o archivos adjuntos de fuentes desconocidas.**
- **Utilice medidas de cifrado para proteger todas las comunicaciones al interactuar con servicios en línea.** [Proyecto Upskill, módulo 4, tema 4.0]. El cifrado es vital para proteger todas las comunicaciones al interactuar con servicios en línea. Sin cifrado, los agentes de amenazas pueden explotar canales no cifrados o no autenticados para inyectar programas maliciosos en los dispositivos de los usuarios, lo que plantea riesgos importantes para la privacidad y la seguridad. Para mitigar estos riesgos, los usuarios deben priorizar el acceso a sitios web y servicios a través de HTTPS, que cifra los datos intercambiados entre el dispositivo del usuario y el servidor del sitio web, y, de este modo, proteger contra las escuchas y la manipulación por parte de agentes malintencionados. Por otro lado, el uso de aplicaciones de mensajería cifradas mejora aún más la seguridad al garantizar que los mensajes y las llamadas permanezcan intactos, confidenciales e inaccesibles para partes no autorizadas.
- **Seleccione las aplicaciones con cuidado.**
  - **Utilice tiendas de aplicaciones confiables** para evitar posibles amenazas de aplicaciones maliciosas de terceros.
  - **Verifique minuciosamente los detalles de la aplicación y la información del desarrollador** antes de descargarla, a fin de mitigar los riesgos potenciales en la fuente.
  - **Examine las aplicaciones de terceros** y asegúrese de que cumplan con los estándares de ciberseguridad [Proyecto Upskill, módulo 1, tema 1.4].
- **Revise y restrinja periódicamente los permisos de las aplicaciones** para minimizar la exposición de los datos, lo que mejorará la seguridad general [Proyecto Upskill, módulo 1, tema 1.3].
- **Mantenga las aplicaciones y el sistema operativo actualizados** [Proyecto Upskill, módulo 1, tema 1.1].

  - **Instale las actualizaciones lo antes posible** para evitar que las amenazas de los agentes de amenazas exploten las vulnerabilidades.
  - **Habilite las actualizaciones automáticas del sistema operativo y de las aplicaciones** para un mantenimiento proactivo de la seguridad.
- **Considere la posibilidad de reiniciar su dispositivo móvil todas las semanas** para eliminar potencialmente los programas espía instalados. Algunos dispositivos móviles ofrecen la posibilidad de programar reinicios, lo que permite establecerlos a una hora determinada, con opciones de programación que van desde intervalos diarios a semanales.
- **Mantenga hábitos seguros de navegación y gestión de la huella digital.**
  - Para iPhones/iPads, **habilite la dirección wifi privada de iOS.** En un entorno de objetivos de alto riesgo, considere la posibilidad de activar el **modo de bloqueo de iOS.** Para obtener más información sobre el modo de bloqueo de iOS, visite la página web Soporte técnico de Apple: acerca del modo de bloqueo.
  - **Considere la posibilidad de emplear soluciones de aislamiento remoto del navegador** para mejorar la seguridad de la navegación web durante investigaciones confidenciales.
  - **Utilice una cuenta de usuario estándar para navegar y otras tareas habituales** [Proyecto Upskill, módulo 1, tema 1.0].

Fabricantes de software

Las agencias autoras animan encarecidamente a los fabricantes de software a comprometerse públicamente y poner en práctica el compromiso de seguridad desde el diseño. Este compromiso implica adoptar los principios de seguridad desde el diseño, que incluyen (1) asumir la responsabilidad por los resultados de seguridad del cliente, (2) adoptar una transparencia radical y una responsabilidad inquebrantable, y (3) liderar desde los niveles superiores e implantar un liderazgo descendente para impulsar cambios transformadores destinados a dar prioridad a la seguridad en todas las fases de desarrollo e implementación del software. Las mitigaciones para mejorar la postura de seguridad de sus clientes incluyen las siguientes:

- **Gestión de vulnerabilidades. Trabajar para eliminar clases enteras de vulnerabilidades en sus productos** con el fin de reducir las posibilidades de que se pongan en peligro. Los agentes cibernéticos maliciosos a menudo explotan debilidades bien conocidas en el software para distribuir sus cargas útiles a través de programas maliciosos. Los fabricantes deben esforzarse por eliminar estas clases de vulnerabilidades en sus productos para evitar que se pongan en peligro.
- **Habilitar la MFA de forma predeterminada en todos los productos.**
- **Proporcionar registros sin coste adicional para el cliente y avisarle** de comportamientos sospechosos o anómalos en sus redes.
- **Implementar alertas que llamen la atención para que los clientes estén al tanto de configuraciones inseguras,** comportamientos sospechosos y cuándo estén descargando programas maliciosos.
- **Incluir detalles de un programa seguro desde el diseño en los informes financieros corporativos.**

Información de contacto

Organizaciones de EE. UU.: Para denunciar actividades sospechosas o delictivas relacionadas con información que se encuentra en esta guía conjunta, utilicen los siguientes contactos:

- Comuníquense con el Centro de Operaciones de la CISA, el cual está disponible las 24 horas, los 7 días de la semana, enviando un correo electrónico a Report@cisa.gov o llamando al (888) 282-0870, o bien, comuníquense con su oficina local de la FBI . 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.

Organizaciones de Canadá: Para denunciar incidentes, envíen un correo electrónico al CCCS a contact@cyber.gc.ca.

Organizaciones de Estonia: Para reportar incidentes de ciberseguridad, envíen un correo electrónico a cert@cert.ee o llamen al +372 663 0299.

Organizaciones de Finlandia: Comuníquense con el NCSC-FI enviando un correo electrónico a ncsc@ncsc.fi o reporten incidentes en https://www.kyberturvallisuuskeskus.fi/en/report.

Organizaciones de Japón: Para reportar incidentes relacionados con esta guía, visiten https://www.kantei.go.jp/jp/forms/nisc_opinion.html (NISC) o envíen un correo electrónico a info@jpcert.or.jp (JPCERT/CC), y para denunciar una actividad delictiva, visiten https://www.npa.go.jp/bureau/cyber/soudan.html (NPA).

Organizaciones del Reino Unido: Para denunciar un incidente importante de seguridad cibernética, ingresen a ncsc.gov.uk/report-an-incident (vigilado las 24 horas). Para recibir asistencia urgente, llamen al 03000 200 973.

Recursos

Consulte el Proyecto Upskill de la CISA para obtener orientaciones detalladas sobre cómo mejorar su postura de ciberseguridad y aumentar el costo, en términos de tiempo y recursos, para que un agente de amenazas se dirija a usted.

Consulte la página web de ejercicios y capacitación en materia de ciberseguridad de la CISA para que la formación en ciberseguridad esté a disposición del público en general.

Para obtener más información sobre los esfuerzos de la FBI para combatir la represión transnacional y acceder a recursos en más de 60 idiomas, visite nuestro sitio. Si cree que puede ser víctima de tácticas represivas, comuníquese con nosotros al 1-800-CALL-FBI o visite el sitio tips.fbi.gov.

Para obtener más información sobre los planes de respuesta a incidentes y de recuperación, consulte los siguientes recursos:

- CISA: Fundamentos del plan de respuesta a incidentes y Manual de respuesta a incidentes y vulnerabilidades de ciberseguridad del Gobierno federal. (Aunque están adaptados a las agencias de la rama civil federal de Estados Unidos [FCEB, por sus siglas en inglés], estos manuales proporcionan procedimientos operativos para planificar y llevar a cabo actividades

de respuesta a incidentes y vulnerabilidades de ciberseguridad, y detallan los pasos para la respuesta a incidentes y vulnerabilidades).

- Centro Nacional de Ciberseguridad de Estonia (NCSC-EE): Para informarse sobre ciberseguridad y prevención, visite https://www.ivaatlik.ee/.

Acceda a la Línea de Ayuda de Seguridad Digital de Access Now y al Laboratorio de Seguridad de Amnistía Internacional para recibir apoyo práctico para los defensores de los derechos humanos y los miembros de la sociedad civil. Envíe un correo electrónico a Cisco para obtener ayuda a no-spyware@external.cisco.com.

Si experimenta una emergencia digital, la Línea de Ayuda de Seguridad Digital de Access Now y el Laboratorio de Seguridad de Amnistía Internacional ofrecen apoyo práctico a los defensores de los derechos humanos y a los miembros de la sociedad civil que crean ser objeto de un ataque.

Si cree que ha sido víctima de un programa espía, también puede enviar un correo electrónico a Cisco para solicitar ayuda a no-spyware@external.cisco.com.

Descargo de responsabilidad

La información presentada en este informe se proporciona “tal como está” solo con fines informativos. Las agencias autoras no respaldan ninguna entidad comercial, producto, empresa ni servicio, incluidas las entidades, los productos o los servicios vinculados en este documento. Cualquier referencia a entidades comerciales específicas o productos, procesos o servicios mediante marcas de servicio, marcas comerciales, fabricantes o de otro modo no constituye ni implica respaldo, recomendación o favoritismo por parte de las agencias autoras.

Agradecimientos

Atlantic Council, Authentic8, Cisco Talos, Cloudflare, CrowdStrike, IBM y Meta contribuyeron a la elaboración de esta guía.

Apéndice A: Agentes patrocinados por el Estado

Según los informes de la industria, los ataques contra las HRC patrocinados por el Estado provienen principalmente de los Gobiernos de Rusia, China, Irán y Corea del Norte. ** Sin embargo, la investigación de un grupo de expertos sugiere que muchos otros países también aprovechan tácticas de represión transnacional digital, que se centran en castigar y silenciar a los disidentes.

Entre los grupos conocidos por atacar a organizaciones de la sociedad civil figuran los siguientes:

- **Velvet Chollima:** grupo vinculado a la República Popular Democrática de Corea (DPRK, por sus siglas en inglés) que realiza ciberespionaje. Velvet Chollima ataca principalmente a periodistas que informan sobre asuntos de la Península de Corea y a investigadores que se centran en la política de Asia Oriental dentro de NGO, grupos de expertos e instituciones académicas.[10]
    - **Alias:** Kimsuky, THALLIUM, Black Banshee, Emerald Street
- **Mustang Panda:** grupo afiliado a la República Popular China (PRC, por sus siglas en inglés) que se centra en el espionaje político. El grupo ataca ampliamente a NGO, instituciones religiosas, grupos de expertos y grupos de activistas en diversos lugares geográficos, entre ellos Estados Unidos, Europa, Taiwán, Hong Kong, Tíbet, Myanmar, Mongolia, Vietnam, Afganistán, Pakistán, India y otros. Su principal objetivo gira en torno a la vigilancia meticulosa de las actividades de las víctimas, junto con el esfuerzo deliberado por empañar e impugnar su reputación.[11] Las tácticas de Mustang Panda subrayan su eficacia a la hora de ejecutar campañas de espionaje político prolongadas y selectivas.
    - **Alias:** BRONZE PRESIDENT, TA416, RedDelta
- **Charming Kitten:** grupo asociado con el Gobierno de Irán que se especializa en atacar a disidentes políticos, organizaciones de derechos humanos, medios de comunicación y académicos involucrados en estudios iraníes para extraer inteligencia a través del ciberespionaje. Según el Equipo de Respuesta ante Emergencias Informáticas en Persa (CERTFA, por sus siglas en inglés), un equipo de respuesta a emergencias informáticas que se especializa en rastrear a los agentes iraníes de amenazas cibernéticas, se ha observado que Charming Kitten ataca a "personas, académicos, periodistas, activistas, grupos de expertos, sectores militares y gubernamentales de los Estados Unidos, Europa y Medio Oriente desde 2014".[12] Entre agosto de 2020 y mayo de 2021, IBM X-Force documentó el éxito de Charming Kitten a la hora de atacar a varias víctimas del movimiento reformista iraní. Esta campaña se centró estratégicamente en la infiltración en cuentas personales de correo electrónico y redes sociales, en consonancia con los objetivos de vigilancia previos a las elecciones presidenciales de junio de 2021 en Irán.[13]
    - **Alias:** TA453, COBALT ILLUSION, Magic Hound, ITG18, Phosphorus, Newscaster, APT35, Mint Sandstorm

** La industria y el Gobierno realizan un seguimiento de los grupos de actividad utilizando diversas metodologías analíticas; identifican la actividad que se considera que procede del mismo grupo de agentes dándole un nombre. Algunos grupos tienen varios nombres o se solapan en parte porque las organizaciones pueden hacer un seguimiento independiente de la actividad. Por lo general, el término "amenaza persistente avanzada" (APT, por sus siglas en inglés) se utiliza para grupos con buenos recursos y patrocinados por el Estado que participan en actividades sofisticadas, a menudo dirigidas y orientadas a la intrusión prolongada en redes o sistemas. Para obtener más información, consulte la página web de la CISA sobre agentes cibernéticos de Estados-nación y attack.mitre.org/groups.

- **Earth Empusa:** identificado como un grupo patrocinado por el Estado de la PRC cuyo enfoque principal es vigilar a activistas, periodistas y disidentes, particularmente entre los uigures que residen en el extranjero en países como Turquía, Kazajistán, Estados Unidos, Siria y Australia.[14]
    - **Alias:** POISON CARP[15], Evil Eye[16]
- **Ejército Electrónico Sirio (SEA, por sus siglas en inglés) o APT-C-27:** grupo centrado en ejecutar operaciones selectivas contra organizaciones humanitarias, periodistas y disidentes, en particular aquellos afiliados al Ejército Sirio Libre contra el régimen.[17]
- **MIDNIGHT BLIZZARD:** el Servicio Ruso de Inteligencia Exterior (SVR, por sus siglas en inglés) ataca principalmente a redes gubernamentales, grupos de expertos, organizaciones de análisis de políticas y empresas de tecnología de la información. Estos agentes recurren a múltiples vías de acceso inicial. Entre ellas se incluyen técnicas de bajo esfuerzo como la suplantación de identidad dirigida por correo electrónico y los servicios de mensajería de terceros dirigidos tanto a cuentas corporativas como personales, así como la explotación de dispositivos web vulnerables y las capacidades de conexión remota. Los atacantes pueden aprovechar las redes privadas virtuales. Cuando tienen éxito, estas técnicas de bajo esfuerzo y alta recompensa permiten a los agentes de amenazas robar información confidencial, adquirir credenciales de usuario y obtener acceso persistente a las redes de las víctimas.
    - **Alias:** APT 29

Apéndice B: Tácticas y técnicas de los agentes patrocinados por el Estado

Para las agencias autoras, comprender el comportamiento de los agentes cibernéticos maliciosos suele ser el primer paso para proteger las redes y los datos. Para las organizaciones con buenos recursos, el éxito que tengan los defensores de la red en la detección y mitigación de operaciones cibernéticas maliciosas depende de esta comprensión.
Aunque las organizaciones de la sociedad civil pueden carecer de personal de defensa de la red interna, comprender los comportamientos maliciosos les permitirá tomar decisiones informadas sobre la asignación de recursos para los controles básicos de ciberseguridad con el fin de mitigar la actividad patrocinada por el Estado.

Este apéndice proporciona una descripción general de las operaciones cibernéticas que permiten a los agentes recopilar información para ataques futuros y luego obtener acceso a redes empresariales o dispositivos móviles con fines de vigilancia y control, o para conocer la misión, los intereses y los contactos del objetivo. La actividad se asigna al marco MITRE ATT&CK, una base de conocimientos accesible globalmente sobre comportamientos cibernéticos maliciosos, donde el comportamiento se clasifica en tácticas y técnicas definidas††:

- **Las tácticas** representan el "por qué"; en otras palabras, los objetivos técnicos, las metas finales y los motivos de los agentes cibernéticos maliciosos para realizar sus acciones.
- **Las técnicas** representan "cómo" un adversario logra un objetivo táctico al realizar una acción.

MITRE ATT&CK se organiza en tres marcos de "dominios tecnológicos" o el ecosistema dentro del cual operan los agentes: sistemas de control empresarial, móvil e industrial.‡‡ Este apéndice proporciona una descripción general de las tácticas y técnicas contra organizaciones de la sociedad civil para los marcos empresarial y móvil, versión 14.

Sistema de control empresarial

Táctica: reconocimiento [TA0043]

Definición: Los agentes cibernéticos recopilan información que pueden utilizar en operaciones futuras.

Descripción de técnicas de reconocimiento conocidas: los agentes patrocinados por el Estado utilizan investigaciones de código abierto para recopilar información, y la naturaleza inherentemente pública de muchas organizaciones de la sociedad civil y de su personal las expone a mayores riesgos. En concreto, las organizaciones y personas de la sociedad civil suelen tener una importante presencia en línea a través de sitios web corporativos, promoción en redes sociales, publicaciones geopolíticas y comunicados de prensa. Los agentes patrocinados por el Estado utilizan esta información para hacer lo siguiente:

- Determinar el alcance y las prioridades de los objetivos posteriores al ataque.

†† En la cibercomunidad, los comportamientos maliciosos se definen comúnmente como tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés).

‡‡ Para obtener más información, consulte: attack.mitre.org y la guía conjunta Prácticas recomendadas para la asignación de MITRE ATT&CK.

- Identificar objetivos, incluidas personas, para posibles campañas de suplantación de identidad.
- Recopilar información del dispositivo y de la red, como direcciones IP y sistemas operativos.

Los agentes de amenazas también utilizan la suplantación de identidad, una forma de ingeniería social, para robar credenciales de inicio de sesión para el acceso inicial a la red. En estos casos, dichos agentes se hacen pasar por fuentes confiables (por ejemplo, colegas, conocidos u organizaciones) para atraer a las víctimas y hacer que proporcionen sus credenciales de inicio de sesión, a menudo introduciendo las credenciales en un sitio controlado por un agente de la amenaza para capturarlas.

Los agentes patrocinados por el Estado invierten mucho tiempo y recursos en la elaboración de identidades para intentos de suplantación de identidad, lo que lleva a intentos meticulosamente personalizados (esto se conoce específicamente como "suplantación de identidad dirigida").
Si bien se ejecutan en su mayoría por correo electrónico, los agentes de amenazas adaptan sus tácticas a las preferencias de comunicación de las comunidades de alto riesgo, y aprovechan los mensajes de texto, las plataformas de redes sociales y los diversos canales digitales utilizados para la investigación y la promoción.

Ejemplo de Velvet Chollima: Velvet Chollima realiza reconocimientos para recopilar información sobre la misión, los intereses y los contactos profesionales del objetivo. Como parte de su reconocimiento, Velvet Chollima ha engañado a los usuarios para que introduzcan sus credenciales en una página web fraudulenta que se asemeja a la página de inicio de sesión de Google. De esta manera, obtuvo los datos de inicio de sesión de la víctima, lo que le permitió acceder a actividades posteriores.

Asignación de MITRE ATT&CK: Consulte la Tabla 1 para ver las técnicas de reconocimiento conocidas asignadas al marco empresarial de MITRE ATT&CK.

Tabla 1: Técnicas de reconocimiento de MITRE ATT&CK

Título de la técnica	Identificación	Descripción
Recopilar información sobre la organización de la víctima	T1591	Los agentes malintencionados recopilan información sobre la organización objetivo (o la organización de las personas objetivo) que puede utilizarse para operaciones futuras.
Búsqueda de páginas web/dominios abiertos	T1593	Los agentes malintencionados buscan en sitios web o dominios para obtener información sobre objetivos que se pueden utilizar para operaciones futuras.
Búsqueda de páginas web/dominios abiertos: redes sociales	T1593.001	Los agentes malintencionados buscan en las redes sociales para obtener información sobre objetivos que se pueden utilizar para operaciones futuras.

Título de la técnica	Identificación	Descripción
Recopilar información sobre la identidad de la víctima	T1589	Los agentes malintencionados recopilan información sobre la persona objetivo o el personal de las organizaciones objetivo que puede utilizarse para operaciones futuras. La información sobre identidades puede incluir una variedad de detalles, incluidos datos personales (por ejemplo, nombre de los empleados, direcciones de correo electrónico), así como detalles confidenciales, como las credenciales.
Recopilar información sobre el host de la víctima	T1592	Los agentes malintencionados recopilan información de los servidores de las víctimas (dispositivos, computadoras) que puede utilizarse durante el ataque. La información sobre los servidores puede incluir una variedad de detalles, incluidos datos administrativos (por ejemplo, dirección IP asignada), así como detalles específicos sobre su configuración (sistema operativo).
Recopilar información sobre la red de la víctima	T1590	Los agentes malintencionados recopilan información de las redes de las víctimas que puede utilizarse durante el ataque. La información sobre las redes puede incluir una variedad de detalles, incluidos datos administrativos (por ejemplo, direcciones IP, nombres de dominio), así como detalles específicos sobre su topología y operaciones.
Suplantación de identidad para obtener información	T1598	Los agentes malintencionados envían mensajes de suplantación de identidad para obtener información confidencial (por ejemplo, credenciales de inicio de sesión) que puede utilizarse para operaciones futuras.

Táctica: acceso inicial [TA0001]

Definición: El acceso inicial se produce cuando los agentes cibernéticos maliciosos intentan obtener acceso a una red objetivo.

Descripción de técnicas de acceso inicial conocidas: los agentes de amenazas persistentes avanzadas (APT) utilizan credenciales obtenidas a través de sus intentos de suplantación de identidad (consulte la sección “Reconocimiento”) para obtener acceso a las redes.

Los agentes de APT también aprovechan la suplantación de identidad mediante programas maliciosos para obtener acceso inicial a los objetivos. En dichos ataques, los agentes

malintencionados se hacen pasar por fuentes confiables para inducir a la víctima a interactuar con un hipervínculo malicioso o abrir un archivo adjunto de correo electrónico con el fin de ejecutar programas maliciosos en los sistemas anfitriones. El programa malicioso implementado permite el robo de datos, la vigilancia o las intrusiones cibernéticas avanzadas. **Nota:** La suplantación de identidad a menudo se ve facilitada por la prevalencia de debilidades bien conocidas en el software que los agentes aprovechan para distribuir sus programas maliciosos.

Ejemplos: Los grupos de APT asociados con Irán, China, Corea del Norte y Rusia integran correos electrónicos de suplantación de identidad dirigida en campañas más amplias que apuntan a comunidades de alto riesgo. Estos grupos implementan mensajes personalizados, y muy convincentes, para incitar a los usuarios a interactuar con enlaces o archivos adjuntos.

Velvet Chollima: Se observó a los agentes de amenazas de Velvet Chollima haciéndose pasar por periodistas que buscaban una entrevista o adoptando la apariencia de académicos que solicitaban la participación en encuestas. Al establecer confianza a través de una secuencia de correos electrónicos iniciales, Velvet Chollima introduce tácticamente elementos maliciosos en comunicaciones posteriores, por lo general a través de enlaces o archivos adjuntos engañosos. En particular, estos enlaces con frecuencia ocultan programas maliciosos que proporcionan a Velvet Chollima acceso no autorizado a la computadora personal de la víctima y facilita la vigilancia de sus comunicaciones.

Además, Velvet Chollima estableció reglas de reenvío automático dentro de la cuenta de correo electrónico de la víctima, lo que garantiza un seguimiento continuo de las comunicaciones incluso si se pierde el acceso directo a la cuenta.

Las operaciones de suplantación de identidad dirigida de Velvet Chollima muestran una estrategia de ciberespionaje matizada y selectiva, que emplea ingeniería social y cargas útiles maliciosas para infiltrarse y vigilar las comunicaciones de objetivos de alto valor.

Mustang Panda: El vector de intrusión inicial preferido del grupo son los correos electrónicos de suplantación de identidad, principalmente para implementar troyanos de acceso remoto. Esto facilita el control remoto de la computadora del objetivo, lo que permite una vigilancia integral de las actividades del usuario. Mustang Panda emplea tácticas estratégicas para inducir a los objetivos a hacer clic en enlaces o archivos adjuntos, que a menudo hacen referencia a acontecimientos actuales e incorporan versiones maliciosas de documentos legítimos o robados. Por ejemplo, en enero de 2022, los correos electrónicos enviados a objetivos europeos incluían un archivo adjunto a un informe señuelo de la Comisión Europea (European Commission) y un enlace a un comunicado de prensa de la Unión Europea sobre las prioridades de derechos humanos.

Al obtener acceso inicial, Mustang Panda utiliza técnicas sofisticadas para una vigilancia prolongada y encubierta. En varios casos, el grupo demostró su

capacidad para monitorear y filtrar datos durante períodos prolongados, lo que muestra su capacidad para permanecer sin ser detectado dentro de la red de una organización.

Charming Kitten: Mediante diversas plataformas de comunicación en línea, Charming Kitten ejecuta operaciones avanzadas de ingeniería social. El grupo de APT se hace pasar estratégicamente por un periodista o un empleado de una NGO y entabla conversaciones engañosas con los objetivos para generar confianza antes de desplegar archivos o enlaces maliciosos. En mayo de 2020, IBM X-Force descubrió 40 gigabytes de videos de formación de Charming Kitten, que proporcionaban información sobre sus metodologías para la filtración de datos de plataformas de correo electrónico destacadas.

Asignación empresarial de MITRE ATT&CK: Consulte la Tabla 2 para ver las técnicas de acceso inicial asignadas al marco MITRE ATT&CK.

Tabla 2: Marco empresarial de MITRE ATT&CK: técnicas de acceso inicial

Título de la técnica	Identificación	Uso
Suplantación de identidad	T1566	Los agentes malintencionados envían mensajes de suplantación de identidad para obtener acceso a los sistemas de las víctimas. Los mensajes provocan la ejecución de código o la descarga de programas maliciosos en los sistemas de las víctimas.
Suplantación de identidad: archivo adjunto de suplantación de identidad dirigida	T1566.001	Los agentes malintencionados envían correos electrónicos de suplantación de identidad dirigida con un archivo adjunto malicioso en un intento de obtener acceso a los sistemas de las víctimas.
Suplantación de identidad: enlace de suplantación de identidad dirigida	T1566.002	Los agentes malintencionados envían correos electrónicos de suplantación de identidad dirigida con un enlace malicioso en un intento de obtener acceso a los sistemas de las víctimas. Los enlaces conducen a la descarga de programas maliciosos en el sistema de la víctima generalmente a través de ingeniería social animando a los destinatarios a hacer clic o copiar la URL (esto requiere la técnica relacionada llamada ejecución de usuario [T1204]).

Sistemas de control móviles

Táctica: acceso inicial [TA0027], descubrimiento [TA0032], recopilación [TA0035], y mando y control [TA0037]

Definiciones: El acceso inicial se produce cuando los agentes cibernéticos maliciosos intentan obtener acceso a un dispositivo móvil objetivo. El descubrimiento ocurre cuando los agentes intentan conocer el dispositivo para respaldar sus operaciones. La recopilación sucede cuando los agentes intentan recopilar datos de un dispositivo. "Mando y control" es cuando los agentes intentan comunicarse con los dispositivos atacados para controlarlos.

Descripción de técnicas conocidas: los agentes utilizan la suplantación de identidad para obtener acceso a los dispositivos, a menudo a través de SMS. También utilizan aplicaciones troyanizadas. Los usuarios descargan estas aplicaciones aparentemente legítimas que albergan software malicioso que permite a los agentes acceder a información confidencial del usuario, incluidos registros de llamadas y datos de geolocalización, y tomar control del dispositivo de un usuario.

Después de obtener acceso a los dispositivos, los agentes suelen instalar programas espía en ellos, como Pegasus e Intellexa. Los programas espía son una herramienta comercial que proporciona amplias capacidades de vigilancia, incluido el seguimiento de la ubicación, la captura de imágenes y audio, así como el acceso a archivos y comunicaciones personales.

Ejemplos: Los siguientes ejemplos identifican cómo los agentes patrocinados por el Estado utilizan aplicaciones troyanizadas y programas espía en sus campañas.

Earth Empusa: En 2021, Meta informó que Earth Empusa estableció sitios web engañosos que se asemejaban a tiendas de aplicaciones de Android de terceros. Estas plataformas señuelo albergaban aplicaciones adaptadas a un público uigur (grupo étnico túrquico originario de las regiones generalizadas del centro y este de China, y culturalmente afiliado a ellas), entre ellas una aplicación de teclado, otra de oración y otra de diccionario.

El análisis de TrendMicro reveló que al descargar estas aplicaciones, el dispositivo del usuario se infectaba con un programa malicioso. El software malicioso orquestado por Earth Empusa tenía como objetivo recopilar una variedad de datos confidenciales, incluida información de geolocalización, registros de llamadas y mensajes SMS. Además, el programa malicioso otorgó acceso no autorizado a la cámara, el micrófono y las capacidades de captura de pantalla del dispositivo, lo que ejemplifica las técnicas de vigilancia avanzadas e intrusivas del grupo.

APT-C-27: Para comprometer la seguridad de estas personas, APT-C-27 creó de manera ingeniosa aplicaciones maliciosas, entre ellas una aplicación llamada VPN Secure, junto con versiones señuelo de plataformas de comunicación populares como Telegram y una aplicación de noticias siria. Este uso estratégico de aplicaciones aparentemente inofensivas refleja el método sofisticado de APT-C-27 en su afán por socavar la seguridad y la intimidad de sus objetivos.

APT-C-27 llevó a cabo una segunda campaña dirigida a afiliados del Ejército Libre Sirio y exmilitares. Mediante ingeniería social, el grupo engañó a las personas para que hicieran clic en enlaces que conducían a sitios web engañosos que imitaban servicios populares como Telegram y Facebook.

Asignación móvil de MITRE ATT&CK: Consulte de la Tabla 3 a la Tabla 6 para ver técnicas asignadas al marco móvil de MITRE ATT&CK.

Tabla 3: Marco móvil de MITRE ATT&CK: técnicas de acceso inicial

Título de la técnica	Identificación	Descripción
Suplantación de identidad	T1660	Los agentes malintencionados envían contenido malicioso para obtener acceso a los dispositivos de las víctimas.

Tabla 4: Marco móvil de MITRE ATT&CK: técnicas de descubrimiento

Título de la técnica	Identificación	Descripción
Seguimiento de la ubicación	T1430	Los agentes malintencionados rastrean la ubicación física de un dispositivo.

Tabla 5: Marco móvil de MITRE ATT&CK: técnicas de recopilación

Título de la técnica	Identificación	Descripción
Datos de usuario protegidos: registro de llamadas	T1636.002	Los agentes malintencionados recopilan datos del registro de llamadas.
Datos de usuario protegidos: mensajes SMS	T1636.004	Los agentes malintencionados recopilan mensajes SMS.
Captura de video	T1512	Los agentes malintencionados utilizan las cámaras de un dispositivo para recopilar información mediante la captura de grabaciones de video. También pueden capturar imágenes a intervalos específicos en lugar de archivos de video.
Captura de audio	T1429	Los agentes malintencionados capturan audio, por ejemplo, conversaciones de usuarios, entornos y llamadas telefónicas.
Captura de pantalla	T1513	Los agentes malintencionados utilizan la captura de pantalla para recopilar información sobre un dispositivo objetivo, como aplicaciones que se ejecutan en primer plano, datos de usuario y credenciales.

Tabla 6: Marco móvil de MITRE ATT&CK: técnicas de mando y control

Título de la técnica	Identificación	Uso
Transferencia de herramientas de ingreso	T1544	Los agentes malintencionados transfieren herramientas, archivos o programas maliciosos al dispositivo de la víctima desde un sistema externo.

Referencias

[1] *See* "Microsoft Digital Defense Report 2023," October 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023. Microsoft's *Digital Defense Report 2023* reports APT threat activity against think tanks, NGOs, media, and human rights activists emerging from Russia (Nobelium, Strontium, Seaborgium), China (Nickel, Gadolinium), North Korea (Osmium), and Iran (Phosphorus).

[2] *See* "CrowdStrike Threat Landscape: APTs & Adversary Groups," CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. According to CrowdStrike's Global Threat Landscape, from August 18 to November 16, 2023, APTs from Iran (Charming Kitten), China (Phantom Panda, Aquatic Panda), and North Korea (Velvet Chollima, Ricochet Chollima) represented potential threats to think tanks.

[3] *See* "CrowdStrike Threat Landscape: APTs & Adversary Groups," CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. According to CrowdStrike's Global Threat Landscape, from August 18 to November 16, 2023, APTs from Iran (Static Kitten, Haywire Kitten, Charming Kitten), China (Cascade Panda, Overcast Panda, Aquatic Panda, Emissary Panda), the Russian Federation (Fancy Bear, Gossamer Bear), and North Korea (Velvet Chollima, Ricochet Chollima) represented potential threats to NGOs.

[4] *See* "CrowdStrike Threat Landscape: APTs & Adversary Groups," CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. According to CrowdStrike's Global Threat Landscape, from August 18 to November 16, 2023, a North Korean APT (Ricochet Chollima) and Iranian APT (Charming Kitten) represented potential threats to dissidents.

[5] *See* "CrowdStrike Threat Landscape: APTs & Adversary Groups," CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. According to CrowdStrike's Global Threat Landscape, from August 18 to November 16, 2023, a Russian APT (Fancy Bear) represented a potential threat to nonprofits.

[6] *See* "Project Galileo 9th Anniversary" (Cloudflare Radar, June 5, 2023), https://radar.cloudflare.com/reports/project-galileo-9th-anniv.

[7] *See* Cloudflare Radar, "DDoS Attack Trends for 2023 Q2" (Cloudflare Radar, July 18, 2023), https://radar.cloudflare.com/reports/ddos-2023-q2.

[8] *See* Cloudflare Radar, "DDoS Attack Trends for 2023 Q3" (Cloudflare Radar, October 26, 2023), https://radar.cloudflare.com/reports/ddos-2023-q3.

[9] See "ENISA Threat Landscape 2023," ENISA, October 19, 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[10] *See* CrowdStrike, "Velvet Chollima" crowdstrike.com, February 25, 2023, https://www.crowdstrike.com/adversaries/velvet-chollima/.

[11] *See* "BRONZE PRESIDENT Targets NGOs," Secureworks, n.d., https://www.secureworks.com/research/bronze-president- targets-ngos.

[12] *See* Certfa Lab, "Charming Kitten: 'Can We Have a Meeting?'" Certfa, n.d., https://blog.certfa.com/posts/charming-kitten-can-we-wave-a-meeting/.

[13] *See* "ITG18: Operational Security Errors Continue to Plague Sizable Iranian Threat Group," Security Intelligence, August 23, 2023, https://securityintelligence.com/posts/itg18-operational-security-errors-plague-iranian-threat-group/.

[14] *See* Mike Dvilyanski and Nathaniel Gleicher, "Taking Action Against Hackers in China," *Meta*, April 20, 2021, https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/.

[15] *See* CitizenLab "Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits" September 24, 2019, https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/.

[16] *See* Volexity Blog "Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs" September 2, 2019, https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/.

[17] *See* Mike Dvilyanski and David Agranovich, "Taking Action Against Hackers in Pakistan and Syria," *Meta*, November 16, 2021, https://about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria/amp/.