jamf

Anatomía de un ataque

En el mundo globalmente conectado de hoy en día, los profesionales de la ciberseguridad tienen mucho trabajo contra los actores de amenazas. Mientras que estos últimos solo necesitan explotar una vulnerabilidad o comprometer un conjunto de credenciales para introducirse en las redes de las organizaciones, los primeros deben hacerlo bien todas y cada una de las veces... o correr el riesgo de que un dispositivo o Las credenciales de un usuario que no cumplan la normativa abran la puerta a una filtración de datos.

Como dijo Thomas Jefferson, "el conocimiento es poder". En este caso, ese poder puede dotar a los actores de amenazas de información sobre los fallos de las defensas de una organización o permite a los profesionales de la ciberseguridad comprender la naturaleza de un ciberataque utilizado contra ellos.

Para ello, es necesario analizar cada fase de la cadena de ciberataques y examinar detenidamente la anatomía de un ataque de este tipo. De este modo, usted puede apuntalar los riesgos al mismo tiempo que refuerza las protecciones.

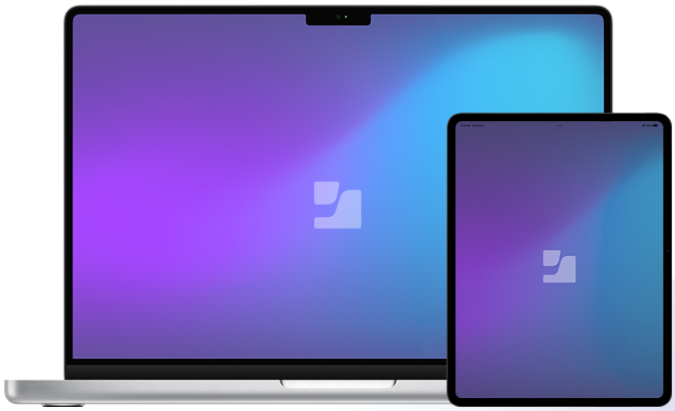
En este documento técnico:

- Analizamos de la cadena de un ataque cibernético
- Demostramos el funcionamiento de un ataque
- Alineamos los eslabones de la cadena con protecciones críticas
- Subrayamos la importancia crítica de cerrar las brechas de seguridad.

Analicémoslo de nuevo

Los ataques varían porque las amenazas que los actores maliciosos deciden incorporar se basan en el objetivo u objetivos seleccionados y en las vulnerabilidades que presentan. Aunque utilizan aspectos similares, la singularidad de los ataques, combinada con las variables que afectan a la seguridad de terminales, es suficiente para hacer de la ciberseguridad una disciplina donde la deducción es tanto arte como ciencia.

Sin embargo, pese a la variedad de amenazas en un ataque, la anatomía de la agresión y los eslabones de la **cadena de ataque cibernético** de Lockheed Martin representan una certeza absoluta. Compuesto por siete fases para alcanzar sus objetivos, que abarcan desde la preparación inicial hasta la ejecución de herramientas maliciosas mediante el análisis de cada fase, los profesionales de la seguridad cibernética pueden identificar los puntos débiles de su armadura en los que los actores maliciosos se enfocarán y crearán vulnerabilidades para eludir las defensas.



"Así que esos son mis esquemas, Y estos son mis planes"

– Tears for Fears

Antes de aprender a leer la hoja de ruta de un atacante, he aquí las siete fases de la cadena de un ataque cibernético:

1.

Reconocimiento
Investigar e identificar objetivos tanto en línea como fuera de línea.

2.

Armamentismo
Utilizar la investigación recopilada para desarrollar y/o adquirir herramientas utilizadas en etapas posteriores.

3.

Envío
Las herramientas maliciosas se utilizan activamente contra los objetivos para obtener acceso.

4.

Explotación
Una vez obtenido el acceso, se aprovechan las vulnerabilidades y otras brechas de seguridad para ampliar aún más el acceso.

5.

Instalación
El despliegue del código malicioso sienta las bases para el éxito de la campaña.

6.

Comando y control:
Se establece la comunicación con los dispositivos comprometidos antes de la fase final del ataque.

7.

Acciones sobre los objetivos
Una vez finalizados todos los preparativos y el trabajo de base, los actores de la amenaza ejecutan las herramientas que llevan a cabo sus objetivos (recopilar información de identificación personal, filtrar datos, ejecutar ransomware, etc.).

¡Es hora del espectáculo!

Echemos un vistazo detallado a cada fase de la cadena de un ataque cibernético. En esta sección, utilizaremos la amenaza de malware distribuida como servicio dirigida a macOS conocida como **Atomic Stealer** (AMOS) como ejemplo de la anatomía de un ataque y de cómo podría llevarse a cabo en un escenario real.

1.

Reconocimiento

En la fase de recopilación de inteligencia, los actores de la amenaza se enfocan exclusivamente en investigar a su objetivo para obtener información detallada sobre la infraestructura de la víctima, la topografía de la red y los proveedores de servicios ascendentes y descendentes. Cualquier detalle les ayuda a crear un perfil de la organización objetivo. Es importante señalar que durante esta fase pueden producirse reconocimientos pasivos y activos.

Activos

Esto puede alertar a las organizaciones que están siendo vigiladas por herramientas invasivas que dejan huellas digitales, como un número excesivo de intentos fallidos de inicio de sesión o huellas en la red.

Pasivos

Se basa en gran medida en el reconocimiento de fuentes abiertas para recopilar información de forma anónima sin avisar al objetivo. Ejemplos de ello son:

- Utilizar las redes sociales para captar víctimas en sectores de alto valor, como las criptomonedas.
- Utilizar las redes sociales para buscar coincidencias de los empleados con sus funciones críticas de la organización de destino.
- Identificación de asociaciones con proveedores para determinar los servicios utilizados por el objetivo para llevar a cabo las funciones empresariales.
- Ingeniería social para engañar a los empleados con el fin de divulgar información sensible o confidencial que pueda utilizarse para aumentar el éxito del ataque.

2.

Armamentismo

Una vez finalizado el reconocimiento, los actores de la amenaza organizan la información que han recopilado y comienzan a personalizar las herramientas que se utilizarán en las primeras fases del ataque. En nuestro ejemplo, los actores de la amenaza realizaron varias tareas para convertir Atomic Stealer en un arma. Desarrollaron el malware y realizaron una firma ad hoc del archivo DMG. Llegaron incluso a proporcionar instrucciones de instalación específicas para que los usuarios pudieran eludir las advertencias de Gatekeeper de Apple. Se creó un sitio web malicioso para imitar el sitio web real del navegador Arc, donde se dirigía a los visitantes a descargar la versión comprometida del software.

NOTA: Durante las fases 1 y 2, las soluciones de seguridad no son especialmente eficaces para detener la cadena de ataques cibernéticos, ya que hasta la fase tres se trata sobre todo de conjeturas. Piénselo así, a diferencia de Minority Report, en las fases 1 y 2 no se producen atentados. Todo lo que existe son pensamientos, ideas o hipótesis en la cabeza de un actor de amenazas. A partir de la fase tres es cuando comienzan los ciberdelitos y debemos esperar a que los actores de la amenaza intenten cometer uno para poder detenerlos.

3.

Envío

Durante esta fase, los actores de la amenaza ponen en práctica sus investigaciones y tácticas.

PASO 1. Lanzamiento de un sitio web de imitación

PASO 2. Se envía a través de anuncios patrocinados en lugar del sitio legítimo de Arc Browser

PASO 3. El usuario descarga y ejecuta el software que compromete la terminal con el malware Atomic Stealer

Debido al alcance de los anuncios patrocinados y a su colocación en los primeros puestos de las búsquedas de los usuarios, tener como objetivo a las personas que usan sus dispositivos, puede propiciar que decenas de terminales queden infectadas en un tiempo relativamente corto. Aunque este ataque en particular no se lanza visitando directamente el sitio web, probablemente sea un medio de eludir la detección. Según Jamf Threat Labs, los ataques que utilizan variantes de Atomic Stealer proliferan rápidamente a medida que las amenazas implementan campañas de phishing por correo electrónico, SMS y redes sociales para llegar a un mayor número de víctimas.

Soluciones como **Jamf Pro** y **Jamf Protect** trabajan conjuntamente para proteger a los usuarios frente a las amenazas. El primero utiliza una combinación de filtrado de contenidos para bloquear las URL de phishing, incluso si los usuarios hacen clic en el enlace. La seguridad de terminales monitorea activamente el estado de los dispositivos y alerta a los administradores de los cambios en el estado de conformidad a medida que los perfiles de inscripción de administración de dispositivos refuerzan la seguridad de los datos, manteniendo los datos empresariales en un volumen cifrado y separado de los datos personales, para evitar que se mezclen. En caso de que los datos empresariales se vean afectados, los administradores pueden automatizar los flujos de trabajo de limpieza de dispositivos, incluyendo la eliminación de datos confidenciales de los dispositivos afectados para evitar su divulgación.

4.

Explotación

Aunque el método de envío de la carga útil puede diferir, según la amplia investigación de Jamf Threat Labs, ***"Su objetivo y lógica, sin embargo, siguen siendo los mismos en última instancia".*** En otras palabras, las credenciales del usuario afectado siguen comprometidas y sus datos sensibles son exfiltrados.

Ese es precisamente el objetivo de Atomic Stealer: el robo de datos de los usuarios tras engañarlos para que introduzcan sus credenciales como parte del proceso de actualizaciones automáticas es, en realidad, una llamada AppleScript basada en el comando 'osascript' nativo de macOS.

Hay que tener en cuenta que, aunque las acciones realizadas en segundo plano por este malware están ampliamente documentadas por **Jamf Threat Labs** (y más adelante en la sección Acciones sobre objetivos), la detección de variantes basadas en este código malicioso, o incluso aquellas desarrolladas de forma única para evolucionar con el tiempo, ofrece a los actores de amenazas la oportunidad de realizar cualquier cantidad de acciones sin que los usuarios sean conscientes de que pueden estar afectados.

Como ser espiado por **amenazas que eluden el marco de Transparencia, Consentimiento y Control de Apple.**

Incluso si las amenazas consiguen comprometer las credenciales de un usuario durante la campaña de phishing, Jamf Trusted Access trabaja para detener otros ataques a lo largo de la cadena de un ataque cibernético mediante la recopilación de telemetría detallada en tiempo real, informando a los administradores de los cambios en el estado de salud del dispositivo. Además, activa la ejecución automática de flujos de trabajo de remediación, como la implementación de actualizaciones para parchar vulnerabilidades, impidiendo que la fase de explotación siga adelante.

En cuanto a las credenciales por sí mismas, **Jamf Connect** administra la identidad y el acceso, lo que permite desactivar las cuentas afectadas hasta que se pueda responder al incidente. Para una **respuesta y recuperación** más rápidas ante incidentes, la integración con Jamf Protect habilita **Zero Trust Network Access** (ZTNA) para minimizar automáticamente el riesgo, identificando cuándo se están utilizando las credenciales afectadas para comprometer otras aplicaciones/servicios. Aísla las amenazas de los servicios afectados, pero impide el movimiento lateral a través de la infraestructura que usted maneja, al mismo tiempo que mantiene la productividad de los usuarios en los servicios no afectados. Por último, cada vez que se realiza una solicitud, se llevan a cabo comprobaciones continuas de hardware y software, lo que proporciona una capa adicional de protección que mantiene desactivado el acceso a los recursos de la empresa por parte de dispositivos y credenciales comprometidos hasta que los flujos de trabajo de verificación corrigen y determinan que los dispositivos afectados se conformen a la normativa.

5.

Instalación

Los actores de amenazas continúan ejecutando código malicioso e implementando malware para establecer su persistencia. Esto mantiene su acceso a los sistemas comprometidos mientras realizan sondeos adicionales para ampliar su alcance mediante movimientos laterales por toda la red a la que están conectados los dispositivos comprometidos, aprovechando herramientas personalizadas y nativas, como utilidades de línea de comandos y código malicioso para crear backdoors (puertas traseras). Como se relaciona directamente con AMOS, ya que su objetivo es simplemente robar toda la información del usuario de una sola vez sin dejar mucho rastro en el sistema, Atomic Stealer toma pasos mínimos en esta etapa. Para otros ataques, normalmente esta fase facilita que las operaciones actuales y futuras se lleven a cabo de forma encubierta.

Es fundamental defenderse de esta fase **aprovechando la visibilidad y la seguridad para garantizar que se mantiene la conformidad** detectando, previniendo y solucionando las amenazas conocidas. El monitoreo activo del estado del dispositivo brinda una alerta a los administradores en caso de que haya cambios en la línea base en la postura de seguridad de un dispositivo, para clasificar y poner en marcha flujos de trabajo de respuesta a incidentes. Jamf Protect impide que se ejecute código malicioso conocido, lo que incluye poner en cuarentena y eliminar las amenazas de malware antes de que puedan ejecutarse. En el caso de las amenazas desconocidas, los registros de los dispositivos se envían a una solución SIEM de terceros para ayudar a los **equipos de caza de amenazas** a detectar y eliminar las amenazas que pudieran estar ocultas en los sistemas, recopilando datos mientras los actores de las amenazas esperan su momento.

6.

Comando y control (C2)

El objetivo de Atomic Stealer es, en primer lugar, robar sus credenciales; en segundo lugar, utilizar estas contraseñas robadas para sustraer sus datos. Pero en función de los objetivos ulteriores del actor de la amenaza, eso no significa que el viaje se detenga ahí. Dado que Keychain ofrece un almacenamiento central y seguro de credenciales, el desguace de este rico recurso suele proporcionar a los atacantes las claves de diversas funciones, software y servicios. Se trata de una perspectiva atractiva para:

- Mayor acceso a recursos ricos en datos
- Ampliar los ataques mediante movimientos laterales
- Ganar más dinero vendiendo y/o extorsionando a las víctimas

En pocas palabras: más datos equivalen a más oportunidades lucrativas.

Evitar la comunicación con dispositivos comprometidos es crucial. ZTNA supervisa las terminales y bloquea las conexiones a servicios maliciosos, como los servidores C2, impidiendo así que los agresores se comuniquen con los dispositivos comprometidos. Además, ZTNA mantiene un monitoreo continuo sobre la integridad de los dispositivos y las credenciales ante cualquier incumplimiento.

De este modo, impide el acceso a recursos protegidos a equipos o identidades comprometidas y restringe el uso de dispositivos no conformes. En paralelo, colabora con Jamf Pro en la ejecución automática de flujos de trabajo para la remediación de dispositivos vulnerables o afectados.

7.

Acciones sobre los objetivos

En esta fase final, los atacantes llevan a cabo toda la amplitud de sus planes, ya sea:

- **Espionaje**
- Exfiltración de datos
- Extorsión
- Ataques a la cadena de suministro
- Ciberterrorismo

O cualquier combinación de ellas; el resultado es el fruto del trabajo del actor de la amenaza. Esta sección es difícil de cuantificar porque al igual que cada organización tiene necesidades únicas, cada atacante basará sus acciones total o parcialmente en sus objetivos únicos. En el caso de Atomic Stealer, el comando 'osascript' mencionado anteriormente, se utiliza para emular la apariencia de una alerta legítima del sistema, pero en su lugar utiliza las credenciales del usuario para recopilar las siguientes formas de datos confidenciales de Apple Keychain:

- Nombres de usuario y contraseñas
- Cookies de sesión del navegador
- Datos sensibles de los usuarios
- Datos de las tarjetas de pago
- Monederos de criptomonedas
- Metadatos del sistema

Repare las grietas de su armadura

Las lagunas de seguridad que dejan las protecciones inadecuadas y el hecho de enfocarse únicamente en los sistemas operativos de escritorio, dejan inseguros a los dispositivos móviles, lo que permite a los actores de amenazas hacerse un hueco en las redes de las organizaciones a través de comprometerlas.

Aunque los dispositivos móviles están lejos de ser el único riesgo que conduce a la violación de datos, el panorama de amenazas en evolución sigue apuntando a los móviles debido a una combinación de mayor adopción en el lugar de trabajo y dispositivos personales cada vez más utilizados para acceder a datos de trabajo. **Las investigaciones de Jamf Threat Labs** cuantifican este riesgo como "el 40% de los usuarios de móviles utilizan un dispositivo con vulnerabilidades conocidas". En los dispositivos vulnerables, los factores de riesgo no controlados permiten a los actores de amenazas:

- Ejecutar código malicioso en dispositivos
- Eludir las protecciones de seguridad internas
- Acceder a datos empresariales no autorizados
- Obtener datos privados sin autorización
- Espiar a los usuarios sin su conocimiento o consentimiento
- Realizar ataques desde el dispositivo infectado para comprometer redes
- Exfiltrar datos personales y empresariales, junto con información sobre privacidad

Apple es conocida por combinar forma y función, estilo y sustancia. Esta filosofía se extiende a un rasgo distintivo de su diseño cada vez más crítico: la seguridad y la privacidad. Los sistemas operativos basados en macOS y iOS incluyen varias protecciones de forma nativa para proteger los dispositivos, los usuarios y sus datos frente a innumerables amenazas, tanto a nivel de hardware como de software.

Los actores de amenazas están evolucionando en sus ataques con nuevas amenazas y variantes de malware emergentes, como la creciente categoría Infostealers. La seguridad basada únicamente en motores de detección de firmas estáticas tiene dificultades para defenderse de amenazas sofisticadas. Algunos, como Atomic Stealer, muestran "cadenas de desarrollo completamente diferentes en lugar de una versión principal que se esté actualizando", según Dark Reading. Por ello, **las amenazas sofisticadas evaden las protecciones integradas** y ponen en peligro los dispositivos, los usuarios y los datos.

"Los hackers solo tienen que acertar una vez; nosotros tenemos que acertar siempre".

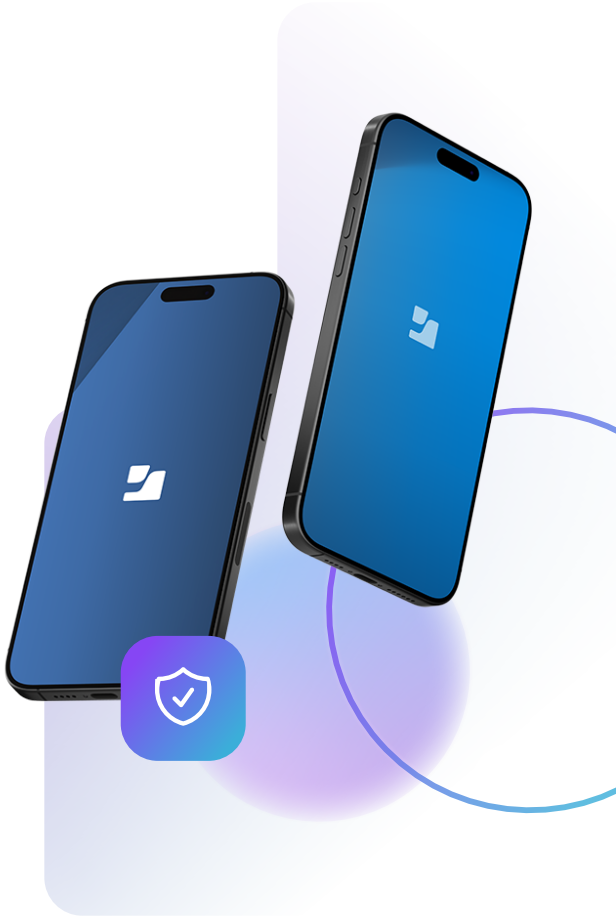
— Chris Triolo, HP

Integre la administración, la identidad y la seguridad en una sola solución, de manera holística. Trabajando juntos —tanto en la red como en el dispositivo— para bloquear de forma exhaustiva el tráfico malicioso. Además, la prevención de la filtración de datos empresariales los mantiene a salvo de los atacantes. ZTNA impulsa este flujo de trabajo impidiendo el acceso a servicios empresariales protegidos al detectar automáticamente cuándo se han puesto en peligro las credenciales y desactivarlas para minimizar el riesgo. Dado que los datos de telemetría se comparten de forma segura e integral, la automatización ejecuta flujos de trabajo para mitigar los vectores de riesgo hasta que se solucionan las vulnerabilidades. Solo después de verificar que las terminales cumplen con los requisitos, se aprueba el acceso a los recursos solicitados.

Los planes de seguridad basados en un **marco de defensa en profundidad**, maduro, son la mejor oportunidad que tienen las organizaciones para mitigar los riesgos, prevenir los ataques conocidos y responder rápidamente a los incidentes con flujos de trabajo de solución automatizados para mantener la conformidad de las terminales.

Mediante la integración y estratificación de soluciones, las organizaciones se defienden contra amenazas sofisticadas con protecciones integrales para "atrapar y mitigar" el riesgo a través de múltiples capas a prueba de fallas. Al mismo tiempo, estas capas de protección se extienden a toda la empresa, proporcionando una base de defensa para todos los tipos de dispositivos y sistemas operativos que soliciten acceso a los recursos y datos de la empresa.

Según un reciente **informe de Frost Radar: Endpoint Security, 2023** sobre las soluciones de Jamf, Frost & Sullivan señaló a Jamf como líder en seguridad de terminales debido a las capacidades de defensa en profundidad de nuestras soluciones:



Detección en tiempo real de aplicaciones maliciosas y scripts, y acciones recomendadas de los usuarios.

Ampliación de la infraestructura de configuración y auditoría para ayudar a los clientes a cumplir con un cumplimiento complejo.

Aplicación consistente de políticas y soporte tanto para dispositivos corporativos como personales.

Administración consistente de vulnerabilidades, prevención de amenazas y control de políticas.

Mayor riqueza de telemetría de terminales para exportar a herramientas de análisis y recopilación de registros de terceros.

Trusted Access de Jamf es la única solución creada específicamente para dispositivos Apple que combina la administración de dispositivos, la identidad y el acceso, así como la protección de terminales.

Informes de seguridad en todas las plataformas Mac y móviles, incluidas macOS, iOS/iPadOS y Android. La protección adicional frente a amenazas web incluye estas plataformas y se extiende a Windows y a Chromebooks.

Conclusión

Mientras las amenazas se sigan dirigiendo a los dispositivos, usuarios y datos, se requerirán controles de seguridad para minimizar los riesgos y evitar que las amenazas conduzcan a violaciones de datos más graves.

El objetivo de un plan de seguridad perenne debe incluir iterativamente:

- Conciencia del riesgo y niveles de tolerancia.
- Implementar capas de mitigación de riesgos y controles de prevención de amenazas.
- Integrar soluciones de administración de dispositivos, identidad y acceso, y seguridad de terminales que funcionen conjuntamente.
- Convergencia entre los equipos de TI y Seguridad para derribar barreras operativas, fomentar la comunicación y tener una respuesta rápida ante incidentes.
- Aprovechar los flujos de trabajo automatizados para remediar las amenazas con rapidez y minimizar los errores introducidos por el usuario.
- Alinear las necesidades y requisitos empresariales con las normas y marcos para reforzar los controles de seguridad y mantener la conformidad.
- Desarrollar un equipo de primera respuesta para agilizar la atención a incidentes; de no ser posible un equipo dedicado, establecer una alianza con profesionales de confianza, como Jamf Threat Labs, para el apoyo en la búsqueda proactiva de amenazas desconocidas.

Asóciese con **Jamf, líder en administración y seguridad de dispositivos Apple**. Aproveche la **experiencia dedicada a la seguridad**, como la de Jamf Threat Labs, para cerrar las brechas en su seguridad mientras implementa flujos de trabajo automatizados para fortalecer su postura de seguridad contra amenazas sofisticadas al mismo tiempo que protege los datos confidenciales, para cada dispositivo que acceda a los recursos protegidos a través de su infraestructura. Independientemente del tipo de dispositivo o sistema operativo, de su ubicación física o de la conexión de red utilizada, **Jamf ayuda a su organización a triunfar con Apple en el trabajo**.