Agosto de 2023

Informe global del panorama de amenazas

Un informe semestral de FortiGuard Labs

FORTINET

Contenido

Resumen ejecutivo

El panorama de amenazas y las superficies de ataque de las organizaciones se transforman constantemente. Además, la capacidad de los cibercriminales para diseñar y adaptar rápidamente sus técnicas para aprovechar la vulnerabilidad de seguridad de este entorno en evolución continúa planteando riesgos significativos para las empresas de todos los tamaños, independientemente de la industria o la geografía.

A medida que examinamos la actividad en la primera mitad de 2023, vemos que las organizaciones de cibercriminales y los grupos ciber-ofensivos de los Estados-Nación adoptan rápidamente nuevas tecnologías. En particular, algunos de estos actores operan de manera muy similar a las empresas tradicionales, con responsabilidades, entregables y objetivos bien definidos. Esta estructura organizacional, combinada con la gran cantidad de recursos que produjeron las vulnerabilidades de seguridad pasadas o de patrocinadores del Estado-Nación, facilita su postura ofensiva, lo que les permite experimentar e incorporar tecnologías que cambian el juego, como la nueva IA generativa, que hace que sus ataques sean más complejos y difíciles de detectar.

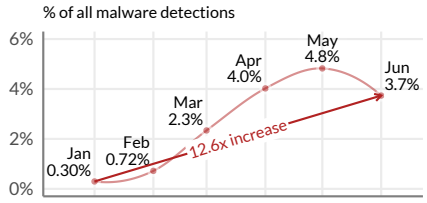
Un aumento significativo en la sofisticación de los actores maliciosos es especialmente evidente en el dominio de la ciberseguridad, donde las amenazas escalaron en frecuencia y complejidad. Esto se caracteriza por un aumento en los ataques altamente dirigidos en varios sectores, incluyendo campañas intrincadas de ransomware, violaciones de datos sustanciales y un cambio notable en las tácticas de MITRE ATT&CK, como se observa a través de nuestras funciones globales de detección mejoradas por IA.

Resumen del primer semestre de 2023

Grupos de APT

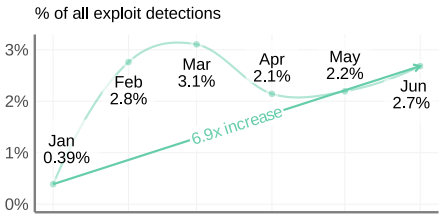
Se detectó actividad en 41 de 138 (30 %) grupos de APT que identificó MITRE. Estos ataques son más enfocados y planificados, además de que se producen en "ondas" rápidas, de modo que es preocupante ver que un tercio de todos los grupos de APT categorizados están activos.

Ransomware



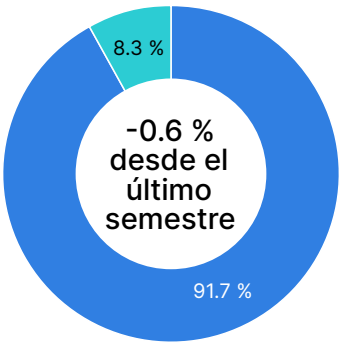
La montaña rusa de ransomware continuó, finalizando el primer semestre de 2023 13 veces más alta de lo que comenzó. Menos organizaciones están detectando ransomware con éxito que en el pasado (13 % frente a 22 %), lo que reafirma que el ransomware también se está volviendo más sofisticado y dirigido.

Ataques de ICS y OT



Los ataques dirigidos a sistemas de control industrial (ICS) y tecnologías operativas (OT) no se produjeron con un gran volumen, pero tendían a aumentar durante el primer semestre de 2023. La mitad de las organizaciones observaron vulnerabilidades de seguridad de ICS u OT, estando entre los principales objetivos la energía eléctrica y los servicios públicos.

Dentro de la zona roja



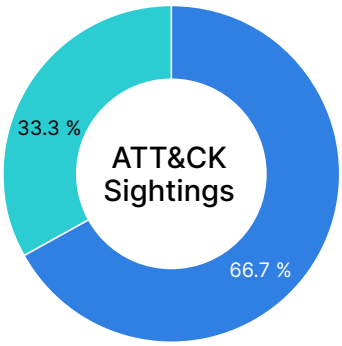
El porcentaje de todas las vulnerabilidades de endpoint con ataque dirigido de los atacantes se mantuvo relativamente estable (aproximadamente el 8 %) en el primer semestre de 2023 en comparación con el período anterior.

Tiempo para aprovechar las vulnerabilidades de seguridad

327 veces

Nuestro análisis muestra que las principales vulnerabilidades que más se pueden aprovechar, según las identifica el EPSS, tienen 327 veces más probabilidades de tener un ataque en una semana que otras en su radar.

ATT&CK Sightings



Con nuestras tecnologías de detección, observamos actividad de dos tercios de todas las técnicas conocidas de MITRE ATT&CK durante el primer semestre de 2023.

En el primer semestre de 2023, observamos una actividad significativa entre los grupos de amenazas persistentes avanzadas (APT), un aumento en la frecuencia y complejidad del ransomware, una mayor actividad de botnets, un cambio en las técnicas MITRE ATT&CK que usan los atacantes y más.

Sin embargo, a pesar del cambiante panorama de las amenazas, no todo son malas noticias para los defensores. En este informe, también analizaremos detenidamente las vulnerabilidades y ofreceremos consejos sobre cómo priorizar sus esfuerzos de corrección y para la aplicación de parches. Adicionalmente, debido a que gran parte de la actividad del panorama de amenazas que vemos es conocido, hay muchas oportunidades para implementar estrategias para defenderse de forma efectiva contra los actores maliciosos. Por último, cubriremos numerosos pasos procesables que puede tomar ahora, como aprovechar la inteligencia frente a amenazas para salvaguardar mejor a su organización.

Un tercio de todos los grupos de APT categorizados estaban activos en el primer semestre de 2023

Vale la pena dedicar un momento para destacar a los actores de amenazas detrás de estas tendencias que analizamos. Como parte de sus esfuerzos para respaldar el marco de trabajo ATT&CK, MITRE rastrea 138 grupos de ciberamenazas.[1] Monitorear la actividad colectiva de estos grupos es un componente esencial para mapear y analizar el panorama de amenazas. De enero a junio de 2023, observamos actividad atribuida a 41 de estos grupos (30 %). De estos, Turla, StrongPity, Winnti, OceanLotus y WildNeutron fueron los más activos, según el análisis del código genético del malware.

Turla es posiblemente uno de los grupos de amenazas más competentes que existen. Han operado bajo numerosos alias (Snake, Venomous Bear y Blur Python, por nombrar algunos) durante casi dos décadas. Turla se relaciona con más de 45 ataques de alto perfil, que afectaron a agencias gubernamentales, medios de comunicación, organizaciones del sector de energía y embajadas en todo el mundo. Han tenido éxito en violaciones de datos de organizaciones y en pasar desapercibidos durante años, incluso en entornos altamente monitoreados, además, dada la escalada del conflicto ruso-ucraniano, no nos sorprendió ver una mayor actividad de este grupo en particular.

Sin embargo, hay algunas buenas noticias: durante los últimos seis meses, la actividad del grupo APT afectó solo a un pequeño subconjunto de todas las organizaciones, lo que indica que la actividad APT continúa siendo muy dirigida, al menos por el momento. Esto tiene lógica ya que no desperdiciarán sus ciberarmas en ataques de pulverización.

La montaña rusa del ransomware continúa

Si bien el ransomware tienen décadas de existencia, en los últimos años fuimos testigos de cómo los actores de amenazas usan cepas más sofisticadas y complejas para infiltrarse en las redes, en gran parte debido al aumento de las operaciones de Ransomware como servicio (RaaS).[2] Además, como la actividad del ransomware continúa siendo desenfrenada, los líderes empresariales de todo el mundo están cada vez más preocupados por esta amenaza. En una encuesta reciente que hizo Fortinet, del 78 % de los líderes que afirmaron que sus empresas estaban preparadas para un ataque, la mitad aún fue víctima de estos.[3]

El ransomware no muestra signos de desaceleración, con una actividad de ransomware que finaliza 13 veces mayor que a principios de 2023, como una proporción de todas las detecciones de malware. No obstante, también estamos en un punto más bajo de la montaña rusa en cuanto a la cantidad de organizaciones afectadas. Casi una cuarta parte (22 %) de las empresas detectaron actividad de ransomware en sus respectivas redes hace cinco años. Actualmente, se redujo al 13 % mientras examinamos la primera mitad de 2023. Desafortunadamente, esta aparente disminución de la actividad no indica que la actividad del ransomware esté disminuyendo. Más bien es una señal de que la distribución de ransomware se volvió más concentrada conforme los grupos de ransomware avanzan en sus modelos comerciales haciendo ataques más dirigidos mediante manuales de estrategias sofisticados y rápidamente adaptables.

La siguiente imagen muestra información sobre las familias de malware más frecuentes que se observaron a través de nuestra telemetría en la primera mitad de 2023. Comparte las principales familias de cada categoría entre criptomineros, infostealers, ransomware y troyanos de acceso remoto (RAT).

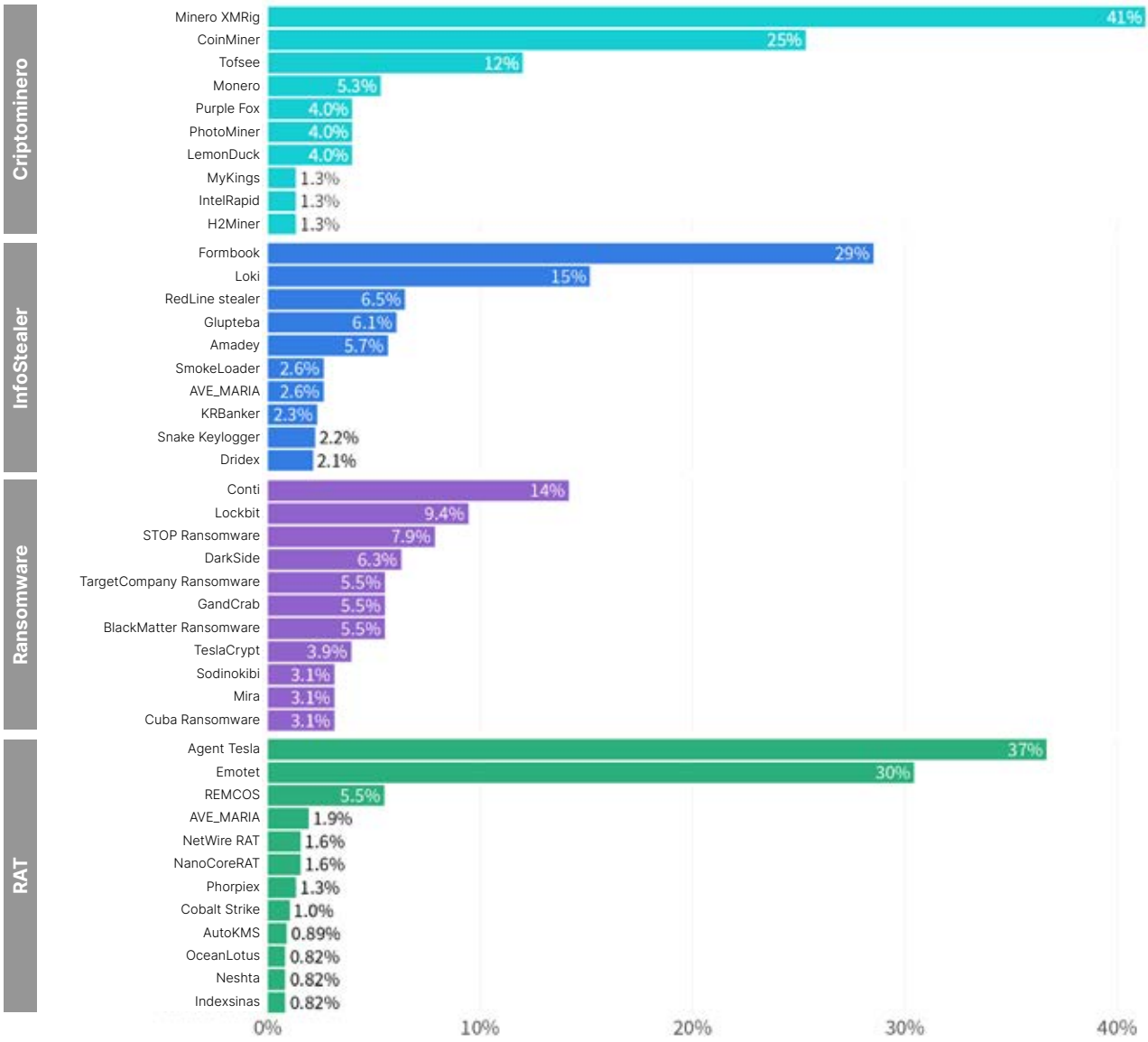


Figura 1: Principales familias de malware por tipo

Los wipers están decayendo... por ahora

Una categoría de ransomware que no aparece en la lista anterior es el malware de wiper.[4] Los wipers se denominan acertadamente porque esta técnica de ataque destructiva "borra" los datos de los sistemas infectados. Observamos un aumento en el uso de wipers a principios de 2022, principalmente junto con el conflicto ruso-ucraniano.[5] A pesar de que ese aumento persistió durante el resto del año, se desaceleró durante el primer semestre de 2023.

Aunque, observamos generalmente que los actores de Estados-Nación usan los wipers principalmente durante tiempos de guerra, también vemos que los cibercriminales usan este tipo de malware para dirigir ataques a organizaciones en sectores específicos, que incluyen tecnología, fabricación, gobierno, telecomunicaciones y atención médica.

Retrocedamos: las tendencias de las amenazas de cinco años

Como profesionales de la seguridad, muchos de nosotros tendemos a suponer que todo siempre empeora con respecto a la ciberseguridad.

No obstante, ¿es esa suposición una realidad o una ficción? Es importante dar un paso atrás ocasionalmente para examinar las tendencias a más largo plazo, esto puede darnos la perspectiva necesaria sobre el estado actual del panorama de amenazas. Retrocedamos y observemos las tendencias de los últimos cinco años con respecto a las vulnerabilidades de seguridad, el malware y las botnets.

Vulnerabilidades de seguridad	Malware	Botnets
10,042 detecciones únicas de vulnerabilidades de seguridad ■ Más de 68 % en los últimos 5 años **54** detecciones de vulnerabilidades de seguridad por organización ■ 75 % en los últimos 5 años **69 %** de las organizaciones observaron ataques severos ■ Menos de 10 % en los últimos 5 años	**44,886** variantes únicas ■ Más de 172 % en los últimos 5 años **7,063** familias diferentes ■ Más de 135 % en los últimos 5 años **18** familias de malware se propagaron a ≥1/10 de todas las organizaciones ■ Más de 100 % en los últimos 5 años	**330** botnets únicas detectadas ■ Más de 27 % en los últimos 5 años **4.3** botnets activas por sensor ■ Más de 126 % en los últimos 5 años **83** días de infección en promedio ■ Más de 1,085 % en los últimos 5 años

Variantes de vulnerabilidades de seguridad en aumento

El conteo de detecciones de vulnerabilidades de seguridad únicas aumentó un 68 % en los últimos cinco años. Por un lado, esto indica que tenemos más formas de detectar ataques maliciosos en el presente que en el pasado. Además, demuestra que los atacantes están multiplicando y diversificando sus vulnerabilidades de seguridad. Sin embargo, al mismo tiempo, observamos una caída del 75 % en los intentos de aprovechar vulnerabilidades de seguridad por organización y una caída del 10 % en las vulnerabilidades de seguridad graves.

Si bien esta caída en los intentos de aprovechar las vulnerabilidades de seguridad puede parecer inicialmente prometedora, es otra indicación de que los atacantes hacen ataques más dirigidos. Las ciberarmas también pueden desgastarse si se usan con demasiada frecuencia, dado que las funciones de detección eventualmente aumentarán, lo que hará que la carga útil se vuelva inútil con el tiempo.

Aumento de la actividad de malware impulsada por el cibercrimen organizado

Las familias y variantes de malware se dispersaron en los últimos cinco años, un 135 % y un 175 %, respectivamente. Podría decirse que es más notable que la cantidad de familias de malware que se infiltró en al menos el 10 % de las organizaciones globales (un umbral crítico de prevalencia) se duplicó. Sin duda, ese es el resultado de un número cada vez mayor de grupos de cibercriminales y de Estados-Nación, así como de la expansión de las operaciones de los que están actualmente activos.

A medida que estos adversarios se vuelven cada vez más selectivos, precisos y destructivos, representan una amenaza progresivamente creciente, lo que requiere una batalla interminable contra ellos. Aprovechando los avances tecnológicos más recientes y significativos de los últimos años, estos enemigos evolucionan rápidamente volviéndose más capaces, versátiles y encubiertos.

Las botnets se vuelven más persistentes

La mayoría de las familias modernas de malware establecieron botnets para la comunicación de comando y control (C2). Dado el crecimiento de las familias y variantes de malware, es lógico que la actividad de las botnet también aumente. En la actualidad, hay más botnets activas (más del 27 %) y una mayor tasa de incidencia de infecciones por botnet entre las organizaciones (más de 126 %).

Sin embargo, el verdadero impulso de las tendencias de botnets es el aumento significativo del número total de "días activos", el tiempo entre el momento en que se detecta por primera vez la actividad de la botnet y la última "activación" del sensor. Esto mide el número promedio de días entre el momento en que detectamos y bloqueamos la comunicación de la botnet antes de que se cambiara el rumbo, después de un intento fallido de violación de datos. Durante los últimos seis meses, eso promedió 83 de 183 días (el último día que medimos), casi la mitad del período. Esto representa un aumento de más de 1000 veces con respecto a las mediciones hechas a principios de 2018, lo que indica que las botnets se volvieron más persistentes en los últimos cinco años. El aumento general en la disponibilidad de vulnerabilidades y las vulnerabilidades de seguridad para incorporar en el "cinturón de armas de la botnet" hace que esto sea un motivo de preocupación, ya que se adaptan rápidamente y aumentan la gama de dispositivos en los que pueden hacer una violación de datos y controlar automáticamente.

Penetrando la Zona Roja

Introdujimos la "Zona roja" en nuestro Informe global del panorama de amenazas del segundo semestre de 2022 para comprender mejor qué tan probable (o improbable) es que los actores de amenazas aprovechen una vulnerabilidad de seguridad de una vulnerabilidad específica.[6]

Si bien varios factores influyen en la relación entre las vulnerabilidades y exposiciones comunes (CVE) en los endpoints y las CVE a las que se dirigen los atacantes, como las prácticas de administración de vulnerabilidades entre las organizaciones o los desarrollos en las herramientas de los adversarios, esto proporciona una imagen valiosa del estado de la superficie de ataque que los líderes de seguridad pueden usar para priorizar sus esfuerzos para aplicar parches.

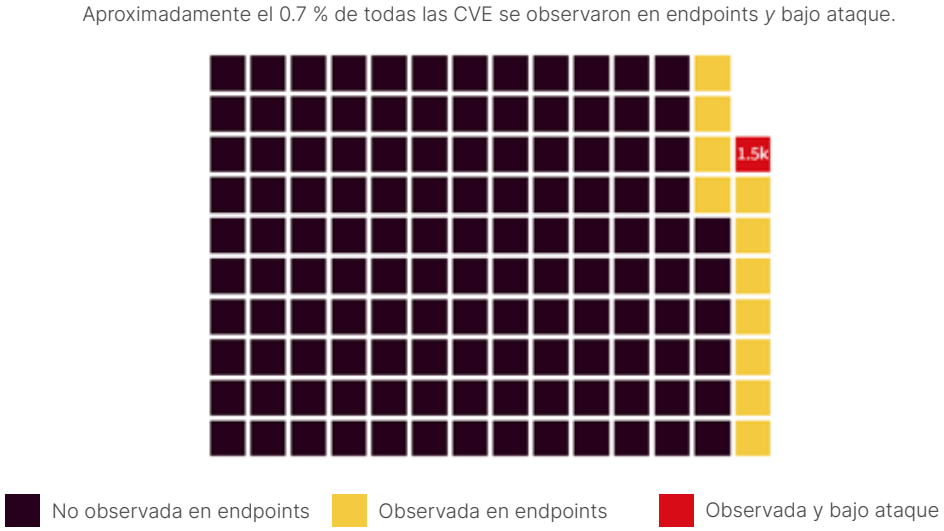


Figura 2: Todas las CVE por presencia en los endpoints y entre ataques

En la segunda mitad de 2022, la zona roja rondaba el 9 %, lo que significa que alrededor de 1,500 CVE, de las más de 16,500 que observamos, estaban bajo ataque. Sin embargo, en el primer semestre de 2023, esta proporción de CVE bajo ataque se redujo al 8.3 %. Curiosamente, apareció aproximadamente la misma cantidad de CVE en ataques, mientras que la proporción de CVE observada en endpoints creció. Si bien esto no indica necesariamente que las organizaciones están ganando terreno en la lucha contra las nuevas vulnerabilidades, al menos el porcentaje de vulnerabilidades bajo ataque parece ser ligeramente menor que en el pasado.

También sabemos que la proporción de vulnerabilidades bajo ataque puede variar ampliamente según la plataforma, hasta un 11 %, como se muestra abajo. Otra distinción notable entre las plataformas es la proporción de todos los CVE que aparecieron en los endpoints, que se muestra en amarillo. Contemple Microsoft y Adobe, donde se observaron más de la mitad de las vulnerabilidades relacionadas, en comparación con el 12 % de las plataformas Apple o el 20 % de Linux. Vale la pena señalar que estas gráficas normalizan todas las plataformas. Por ejemplo, un cuadrado de Adobe representa un número absoluto diferente de vulnerabilidades de Linux.

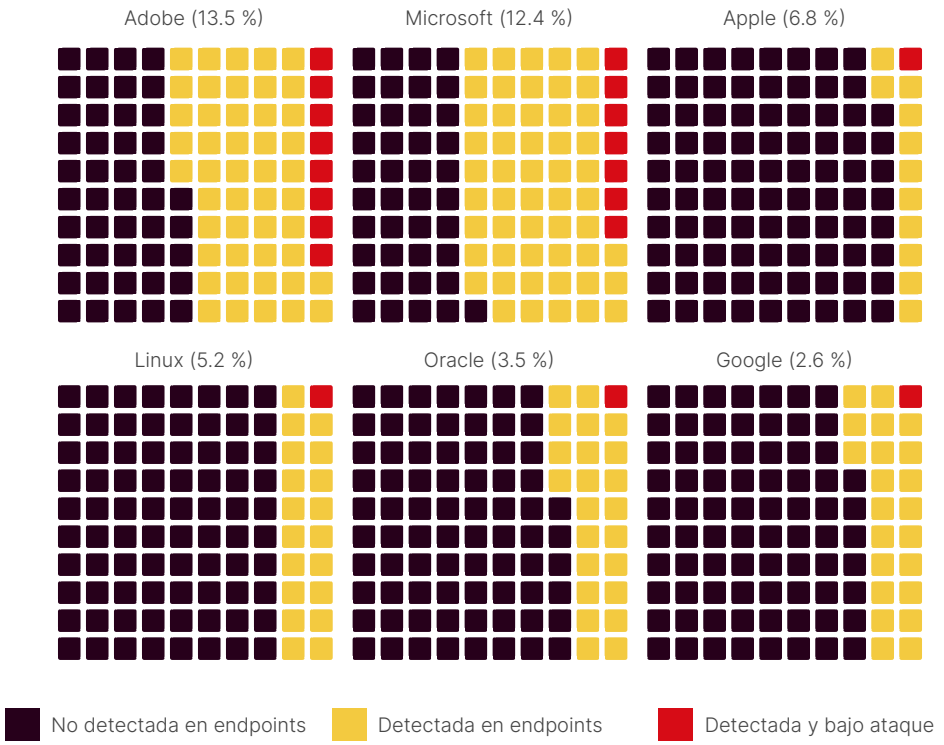


Figura 3: CVE de múltiples plataformas por presencia en endpoints y entre ataques

Lo que está claro es que las organizaciones continúan luchando para desactivar las vulnerabilidades tan pronto como se liberan y los cibercriminales se apresuran para aprovechar la vulnerabilidad de seguridad en esa realidad. Por lo tanto, es vital tener una estrategia sólida para priorizar a qué vulnerabilidades aplicar parches. Si bien cada plataforma se debe considerar durante ese proceso de priorización, eso es solo superficial al anticipar qué vulnerabilidades activas probablemente serán el objetivo de los atacantes en el futuro cercano.

La buena noticia es que los defensores ya tienen algo más poderoso a su disposición, el Sistema de puntuación de predicción de vulnerabilidades de seguridad (EPSS), que se trata en la siguiente sección.[7]

Desde la predicción de vulnerabilidades de seguridad hasta el brote

Desde sus comienzos, Fortinet es un contribuyente importante de datos de la actividad de aprovechamiento de vulnerabilidades de seguridad en apoyo del EPSS. El Sistema de puntuación de predicción de vulnerabilidades usa varias fuentes de datos para predecir la probabilidad de que una vulnerabilidad se aproveche en su entorno libremente. Un grupo de interés especial dirige el Sistema de puntuación de predicción de vulnerabilidades de seguridad en FIRST.org, donde Fortinet es una empresa asociada.

Los equipos de administración de vulnerabilidades usan el EPSS para ayudar a priorizar sus esfuerzos de corrección. Sin embargo, el EPSS también puede respaldar los esfuerzos de inteligencia para rastrear el avance de las vulnerabilidades desde la divulgación inicial hasta el aprovechamiento de la vulnerabilidad de seguridad en su entorno libremente. Este es el caso de uso que queremos explorar aquí. Si los datos de EPSS se incorporan a su proceso de inteligencia frente a amenazas, se pueden usar de forma efectiva como un sistema de alerta anticipada.

Veamos un ejemplo. El 31 de mayo, se anunció una vulnerabilidad de inyección SQL en la aplicación de transferencia web MOVEit que podría permitir que un atacante no autenticado cambie o elimine elementos en el motor de la base de datos que se usa.[8] La comunidad de ciberseguridad reconoció rápidamente esta vulnerabilidad como algo a considerar y FortiGuard Labs lanzó una señal de amenaza para expandir el conocimiento y una firma IPS para monitorear la actividad del uso de la vulnerabilidad de seguridad.[9]

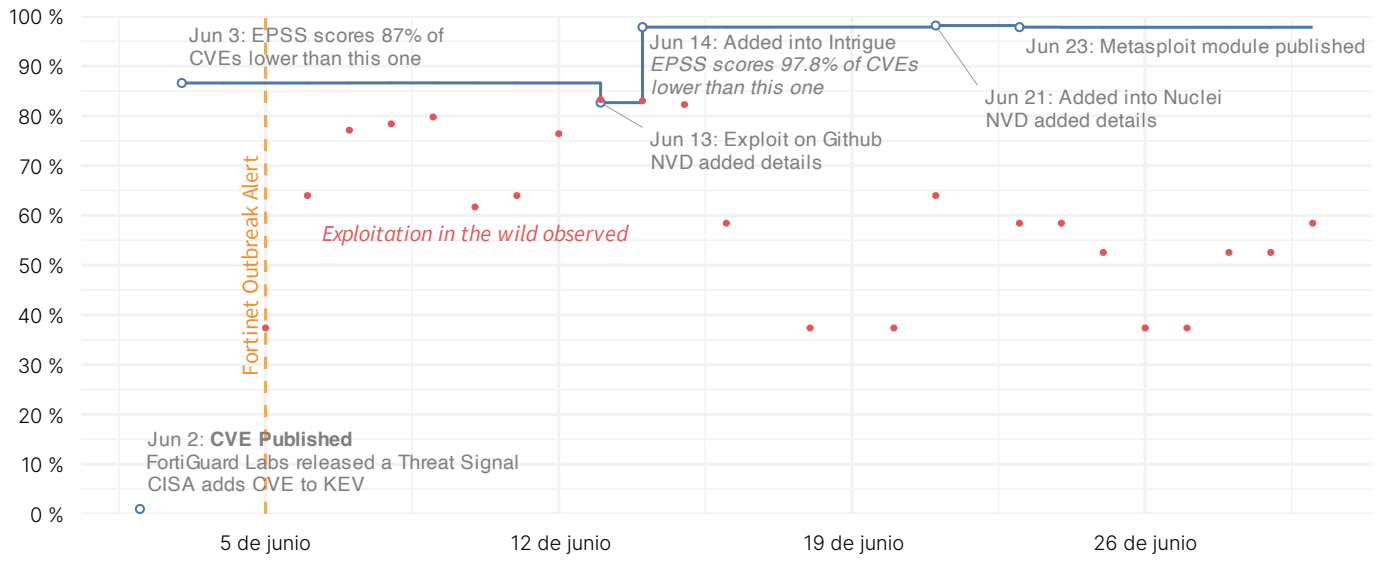


Figura 4: Evolución del EPSS y aprovechamiento de la vulnerabilidad MOVEit

Una vez publicada la CVE, el EPSS pudo predecir una probabilidad muy alta de aprovechar la vulnerabilidad de seguridad en los próximos 30 días. Alerta de spoiler: no tardó mucho tiempo. Nuestros sensores registraron los intentos de los atacantes de aprovechar la vulnerabilidad de seguridad de la vulnerabilidad de MOVEit el 5 de junio, solo cinco días después de que se identificara la vulnerabilidad por primera vez, y publicamos una firma ese mismo día. En este caso, el EPSS dio una validación independiente de lo que anticiparon nuestros analistas y nos ayudó a adelantarnos a esta amenaza emergente durante su rápido período de crecimiento.

El ejemplo de MOVEit genera una serie de preguntas interesantes. ¿Cuánto tiempo tarda generalmente una vulnerabilidad en pasar del lanzamiento inicial a ser aprovechada en el entono libremente? ¿Se aprovechan más las vulnerabilidades de seguridad de las CVE con un puntaje del EPSS alto o aquellas con puntajes más bajos? Si es así, ¿podemos predecir el tiempo promedio para aprovechar la vulnerabilidad de seguridad de cualquier vulnerabilidad dada usando el EPSS?

Veamos si podemos responder esas preguntas. Para hacer eso, analizamos seis años de datos que abarcan más de 11,000 vulnerabilidades publicadas en las cuales nuestros sensores detectaron que se aprovecharon. Con cada CVE, determinamos el tiempo desde la publicación hasta la primera observación de la vulnerabilidad de seguridad y la puntuación EPSS correspondiente. El análisis generado se captura en la gráfica debajo:

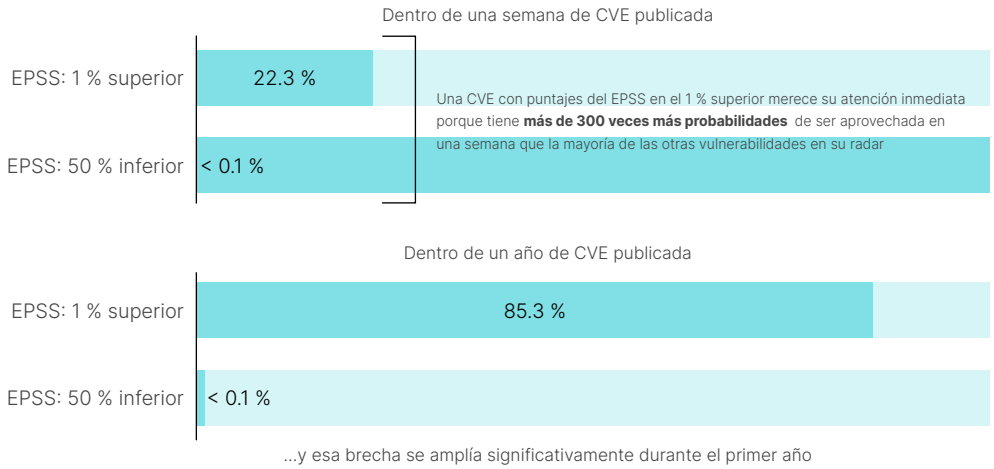


Figura 5: Tasa de aprovechamiento de vulnerabilidades con diferentes puntajes del EPSS

En resumen, aprendimos que el EPSS es importante para predecir qué vulnerabilidades podrían aprovecharse y qué tan rápido ocurrirá esto. Dentro de los siete días posteriores a la publicación, el 22 % de las vulnerabilidades con las puntuaciones del EPSS más altas (el 1 % superior) tuvo actividad de aprovechamiento de la vulnerabilidad de seguridad, en comparación con solo el 0.07 % de las que se encontraban en la mitad inferior de las puntuaciones EPSS. Después de un año completo, el 85 % de las CVE del EPSS con rango más alto registraron el aprovechamiento de la vulnerabilidad de seguridad, mientras que la mitad inferior permaneció en gran medida ignorada por los atacantes.

Eso significa que una CVE con un puntaje del EPSS en el 1 % superior merece su atención inmediata porque tiene 300 veces más probabilidades de aprovecharse en una semana que la mayoría de las otras vulnerabilidades en su radar. Si aún no lo hace, obtenga esos puntajes EPSS diariamente y priorice sus esfuerzos para aplicar parches en consecuencia.[10]

Mapa global de calor de ATT&CK

Después de aproximadamente seis meses de procesamiento continuo de datos usando nuestra red global de más de 10 millones de sensores, compilamos una lista de los hashes más comúnmente observados en el entorno libre. Nuestros avanzados sensores emplean técnicas de aprendizaje automático (ML) para transformar los datos sin procesar en un conjunto de datos enriquecido que examina si hay posibles amenazas en el tráfico de la red. Luego, usamos nuestra cartera de productos y soluciones de Fortinet para analizar las cargas útiles maliciosas detectadas, observando e identificando comportamientos sutiles indicativos de su intención subyacente. Los conocimientos que se obtienen mediante este proceso son cruciales para los defensores de la ciberseguridad en todo el mundo, lo que permite la participación del equipo rojo de enfoque puntual y actividades efectivas de búsqueda de amenazas.

MITRE nos ofrece una mejor comprensión de las operaciones de los actores de amenazas. Tanto fácil de seguir como procesable, ATT&CK permite a los defensores categorizar los comportamientos de los actores de amenazas de una manera sistemática y repetible, lo que finalmente ayuda a los equipos de seguridad a identificar mejor los posibles ataques y evaluar con precisión el riesgo organizacional.

Tenga presente que este informe representa solo “una parte del pastel”. Las diferentes soluciones de seguridad tienen sus propias funciones y tareas únicas con respecto a la detección de técnicas específicas. Este análisis se basa en datos de las soluciones de detección y respuesta de endpoint FortiEDR y sandboxing de FortiSandbox.

Primero examinemos los datos. Estas técnicas se pueden interpretar mejor como funciones de ataque.

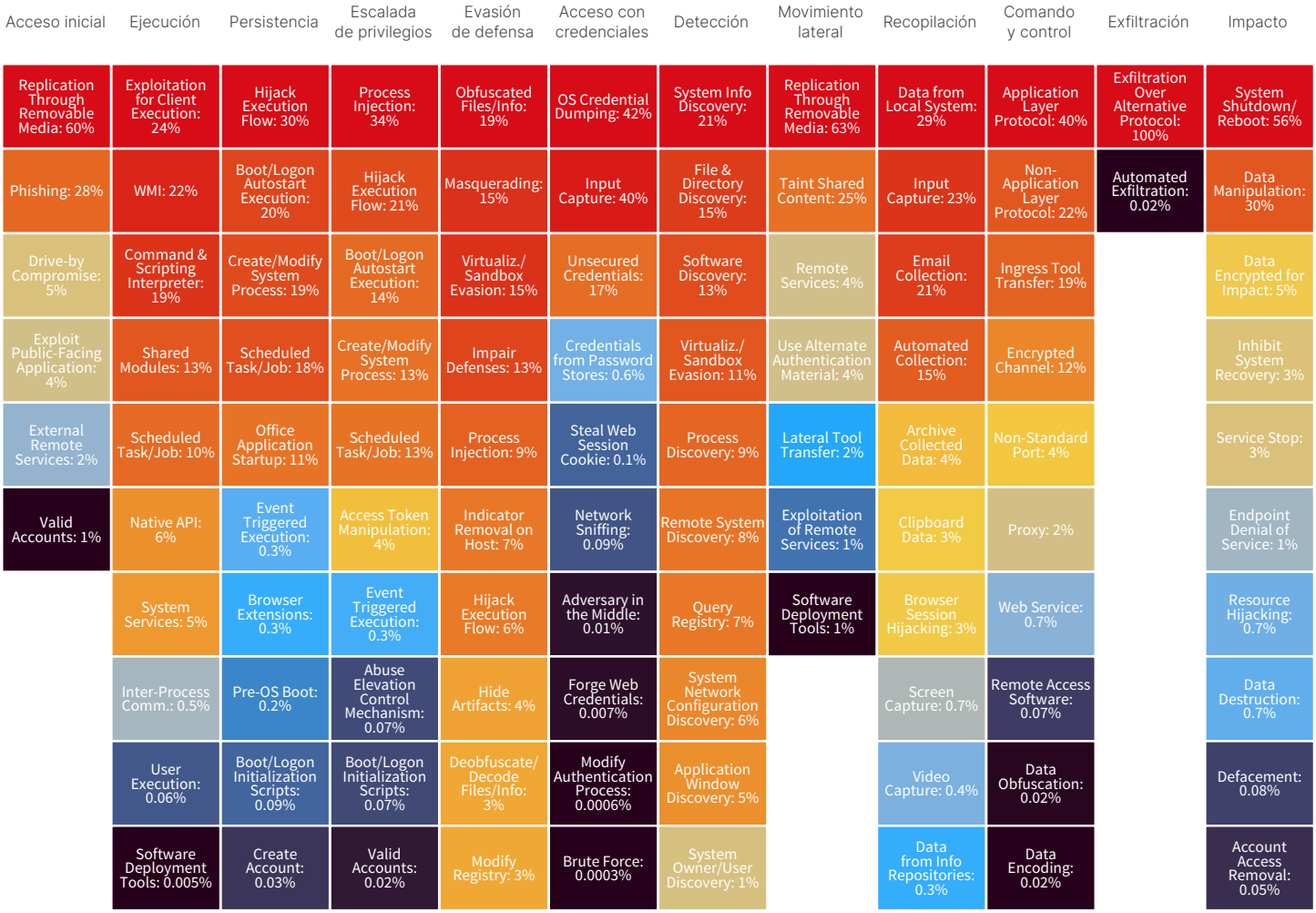


Figura 6: Técnicas ATT&CK para datos en la nube por táctica

Como puede ver, las detecciones obtenidas de los datos dan una visibilidad completa en todo el marco de trabajo de ATT&CK. Las columnas de arriba resaltan las 10 técnicas más detectadas para cada táctica. Las subtécnicas descritas en cada columna de categoría se presentan en su técnica principal por motivos visuales. Exploremos cómo se implementaron estas técnicas en los últimos seis meses y analicemos las formas de contrarrestarlas.

En la fase de acceso inicial, la técnica más predominante que se observa es la replicación mediante medios extraíbles.[11] Aunque no es el punto de entrada número uno a las redes corporativas, la mayoría de las cargas útiles maliciosas que analizamos se podrían propagar a través de este método. En esta técnica se observó un repunte del uso cuando Raspberry Robin la captó, lo que cubrimos en nuestro informe anterior.[12] Desde entonces, Microsoft descubrió muchos otros usos de este gusano, con Raspberry Robin creciendo hasta convertirse en una de las mayores plataformas de distribución de malware. Desde la perspectiva de FortiGuard Labs, este gusano se propagó tan ampliamente principalmente debido a su simple táctica de enmascarar un archivo. LNK como una carpeta, que probablemente la mayoría de las personas abriría. La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) nombró a esta familia de malware como uno de los instaladores de malware más activos que existe, que se usa para distribuir malware IcedID, TrueBot y Bumblebee.[13]

En la fase de ejecución, notamos un aumento en la vulnerabilidad de seguridad de la ejecución del usuario.[14] Esta tendencia implica que los ataques dependen cada vez menos de que los usuarios activen una carga útil o habiliten macros sin darse cuenta. Un ejemplo es una vulnerabilidad específica aprovechada en Microsoft Word, como la vulnerabilidad Follina, cada vez más prevalente, que describimos en varias de nuestras publicaciones de blog recientes.[15]. También observamos esta tendencia en las amenazas que interrumpió FortiEDR. Actualmente, muchas dependen menos de la interacción del usuario para lograr la ejecución del código. Una forma de salvaguardar a su organización de esta técnica es reducir su superficie de ataque aplicando parches las vulnerabilidades con regularidad.

En la fase de Persistencia, continuamos viendo instancias altas de Carga Lateral de DLL (bajo el Flujo de ejecución de Hijack).[16] 3CX empleó esta técnica para lograr tanto Evasión de defensa como Persistencia, las cuales analizamos en esta publicación de blog reciente.[17] Esta técnica es particularmente problemática porque permite a los atacantes eludir medidas de protección como el Application Control y otras limitaciones en la ejecución del software. Para proteger la red de su organización de esta técnica, asegúrese de que el software no sea vulnerable a la carga lateral de DLL en primer lugar, ya que no hay mucho que pueda hacer para evitar la ejecución de un código no deseado. Si bien las cargas útiles maliciosas dentro de la red se marcarán eventualmente, eso solo ocurrirá después de que se carguen en la memoria.

Las tres técnicas principales en la Evasión de defensa no son una gran sorpresa: Archivos e información ofuscados, Enmascaramiento y Virtualización/evasión de sandbox.[18, 19, 20] Incluso piezas únicas de malware demuestran diversas formas de ofuscación, desde las llamadas API hasta las strings en la memoria. Dada la amplia implementación de las soluciones de sandbox en las instalaciones locales y las ofertas de software como servicio (SaaS), el dominio de estas técnicas se vuelve esencial para cualquier actor de amenazas.

El vertido de credenciales del Sistema Operativo y la captura de entrada lideran el paquete en Acceso con credenciales.[21, 22] Desde su lanzamiento, observamos múltiples actores de amenazas que aprovechan Mimikatz para la función relacionada. Además, su integración en varios marcos de trabajo posteriores a la vulnerabilidad de seguridad, como Cobalt Strike, Metasploit y Sliver (y su capacidad para cargarse reflexivamente a través de PowerShell) lo convierten en una herramienta útil, incluso entre ataques sin archivos.

Las fases de Detección y Movimiento Lateral exhiben una relación simbiótica; una mayor detección de activos conduce a un mayor movimiento lateral dentro de entornos comprometidos. Una de las estrategias de defensa más efectivas contra esto es garantizar la visibilidad y el control adecuado sobre el tráfico de la red, ya que durante estas fases se produce una amplia variedad de técnicas que pueden detectarse con los controles adecuados.

De Recopilación a Impacto, poco cambió. Los adversarios usan las mismas técnicas para recopilar y agregar información confidencial, luego se exfiltran a través de un protocolo diferente del canal de comando y control. Aproximadamente el 22 % de los ataques usan una capa que no es de aplicación, como UDP o ICMP, para comunicarse con sus servidores C2. Aunque es una opción inusual debido a la mayor complejidad para establecer y mantener una conexión y una falta de corrección de errores, esta técnica puede pasar desapercibida porque estos protocolos no se monitorean detenidamente.

Información técnica de telemetría de endpoint

Analizar nuestros datos de FortiEDR nos da otra perspectiva con respecto a los ataques y las técnicas de acceso inicial que usan los cibercriminales. En la mayoría de los casos, las organizaciones que usan las funciones EDR también usan alguna forma de sandboxing, por lo que es seguro decir que las amenazas que detiene una herramienta de EDR son probablemente aquellas que habrían logrado eludir la tecnología de sandboxing "tradicional" (un excelente ejemplo de la necesidad de una defensa en profundidad). Comprender cómo operan estas amenazas puede darles a los defensores una inteligencia más enfocada para sus actividades de búsqueda de amenazas.

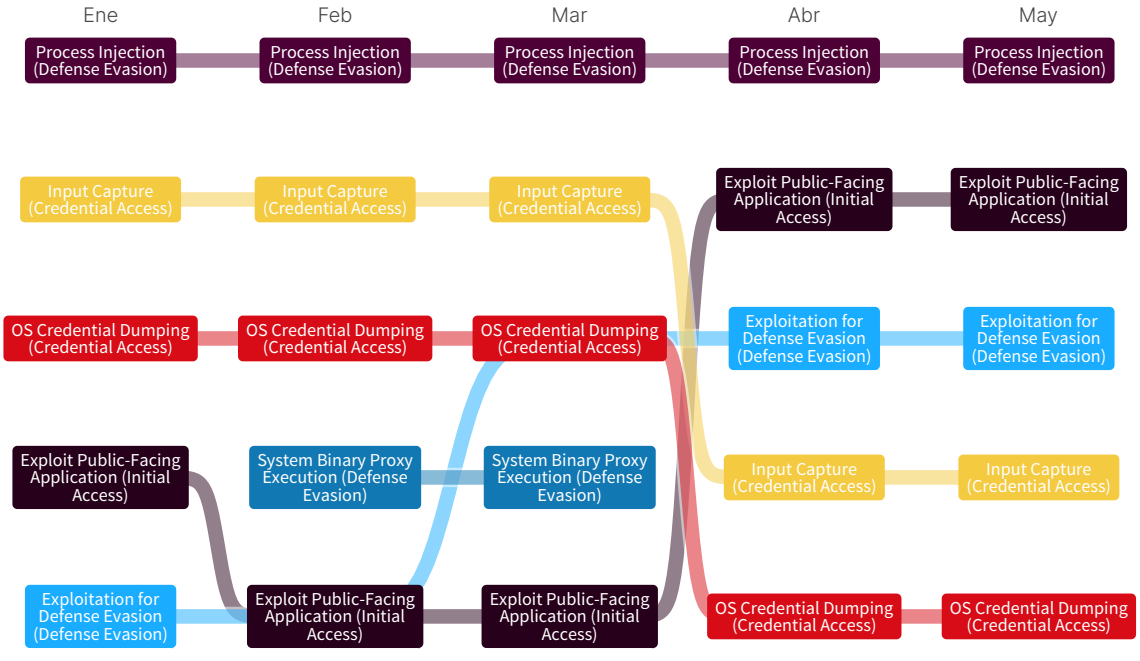


Figura 7: Principales técnicas de ATT&CK que detecta FortiEDR por mes

Arriba están las cinco técnicas más activas por mes. Algunas de las mismas técnicas vistas y detenidas por la tecnología de sandboxing se usan en otros eventos una vez que se logra la ejecución dentro de una máquina en una organización. Las técnicas más activas que observamos durante el primer semestre de 2023 incluyen:

- Inyección del proceso
- Captura de entrada
- Vertido de credenciales del sistema operativo
- Vulnerabilidad de seguridad de la aplicación orientada al público
- Vulnerabilidad de evasión de defensa

El proceso de inyección es lidera todos los meses.[23] Con una docena de posibles tipos de inyección del proceso categorizados, los atacantes sin duda usan y abusan de esta técnica tanto para evadir la defensa como para escalar privilegios.

La segunda y tercera técnicas más usadas en todos los meses es Acceso con credenciales: Captura de entrada. Mediante estas técnicas, los actores de amenazas potenciales intentan interceptar la entrada del usuario para adquirir credenciales o acumular datos buscando credenciales en la memoria. Con frecuencia, durante la interacción regular con el sistema, los usuarios comparten sus credenciales en varios endpoints, como portales de autenticación o ventanas de avisos del sistema. Por lo general, el usuario puede distinguir los mecanismos implementados para capturar esta entrada, como mediante el Enlace de API con credenciales.

Para terminar, tenemos la Vulnerabilidad de seguridad de Evasión de defensa y Acceso inicial como las técnicas finales más usadas, con casi el mismo número de activaciones en el entorno libre. Los adversarios están ansiosos por aprovechar las vulnerabilidades en el software para obtener un punto ventajoso en el sistema para poder hacer sus acciones nefastas. Con el número de CVE creciendo exponencialmente en los últimos dos años (estamos en la ruta para alcanzar las 30,000 CVE este año, un aumento del 50 % sobre las 20,000 CVE informadas en 2021), no es que haya escasez de vulnerabilidades para que los atacantes agreguen a sus respectivas cajas de herramientas. Junto con la llegada de los LLM (modelos de lenguaje grande que se usan para procesar rápidamente grandes conjuntos de datos para identificar rápidamente las amenazas entrantes y las vulnerabilidades existentes), crear una vulnerabilidad de seguridad es más fácil que nunca para estas, por lo que esperamos que continúe siendo el arma que eligen los atacantes.

Protección de su empresa frente a las amenazas en evolución

Los cibercriminales nunca perderán la oportunidad de obtener ganancias, y el aumento del cibercrimen organizad como los grupos RaaS en los últimos años facilita tener un día de pago rápido. Los actores maliciosos encontrarán constantemente nuevas vulnerabilidades que aprovechar y técnicas de ataque más sofisticadas para infiltrarse en las redes. Sin embargo, la buena noticia es que la mayoría de las tácticas que usan los actores de amenazas en los últimos meses nos son conocidas, lo que significa que los defensores tienen más oportunidades que nunca para frustrar los ataques antes de que sucedan.

Sin embargo, a medida que los atacantes continúan desarrollando sus propias operaciones, es fundamental evaluar y mejorar las estrategias de ciberdefensa dentro de su organización para mantenerse a la vanguardia de las posibles amenazas. Desde el uso y el intercambio de inteligencia frente a amenazas hasta la implementación de las tecnologías adecuadas, presentamos varios pasos que puede seguir actualmente para proteger las redes y los datos de su empresa.

Comparta y use la inteligencia frente a amenazas

Para combatir la sofisticación y el volumen cada vez mayores de las ciberamenazas, la práctica de compartir y usar la inteligencia frente a amenazas se convirtió en un componente vital de cualquier estrategia de defensa organizacional. Fortinet está comprometida con hacer su parte para facilitar los avances en el intercambio de inteligencia frente a amenazas.

Fortinet es un miembro fundador de la Cyber Threat Alliance (CTA), una organización creada en 2014 para facilitar el intercambio de inteligencia frente a amenazas entre los proveedores de ciberseguridad de la competencia.[24] El rápido avance actual y esta organización se volvieron vitales para combatir el cibercrimen de forma efectiva a escala global. Sin embargo, el establecimiento de la confianza y la confidencialidad, la garantía de la estandarización de los datos y la administración de un gran volumen de información son solo algunos de los obstáculos que complican el intercambio efectivo de inteligencia. La CTA aborda con éxito estos desafíos, uniendo los equipos de élite de Inteligencia frente a ciberamenazas (CTI) en todo el mundo y mejorando significativamente la perspectiva global sobre las ciberamenazas.

Comprenda los flujos de ataque para identificar patrones e Indicator of Compromise

Los ciberataques son cada vez más sofisticados, frecuentes y dañinos, lo que hace que sea crucial para las empresas mejorar el conocimiento de sus adversarios. Conocer el flujo de ataque, desde los puntos de entrada iniciales hasta las actividades posteriores al aprovechamiento de la vulnerabilidad de seguridad es esencial para desarrollar estrategias de ciberseguridad efectivas.

El flujo de ataque se refiere a la secuencia de pasos que toma un adversario para infiltrarse en un sistema objetivo y lograr sus objetivos. Comprende varias etapas, incluyendo el reconocimiento, el acceso inicial, la escalada de privilegios, el movimiento lateral, la exfiltración de datos y la persistencia. Al conocer cada etapa, las organizaciones pueden identificar mejor las vulnerabilidades, implementar las medidas de seguridad apropiadas y responder de manera efectiva a las ciberamenazas.

Conocer el flujo de ataque es crucial por varias razones. Primero, permite a las organizaciones conocer visualmente los pasos de un ataque, así como sus relaciones y resultados. Al estudiar las tácticas, las técnicas y los procedimientos (TTP) de los adversarios en cada etapa, los equipos de seguridad pueden identificar los patrones y los Indicator of Compromise (IOC), lo que les permite identificar un ataque en progreso y tomar medidas oportunas.

Conocer el flujo de ataque también ayuda a las organizaciones a asignar recursos de manera más efectiva. Con el enfoque en las etapas más vulnerables de un ataque, como el acceso inicial o la escalada de privilegios, las empresas pueden priorizar las medidas de seguridad y las inversiones para maximizar su postura de ciberseguridad.

Por último, conocer el flujo de ataque permite a las organizaciones mejorar sus funciones de respuesta a incidentes. Al mapear las distintas etapas y posibles actividades de un ataque, los equipos de seguridad pueden desarrollar manuales de estrategias y planes de respuesta adaptados a cada etapa, lo que garantiza una respuesta rápida y eficaz durante un ciberataque.

Las ventajas de conocer plenamente los flujos de ataque son la razón por la que Fortinet participa como patrocinador de la investigación de ambos proyectos del Flujo de ATAQUE de MITRE Engenuity's Center for Threat-Informed Defense (CTID).[25] Creemos que estos avances de la inteligencia frente a amenazas, en los que podemos identificar y responder a las amenazas basadas en su perfil, cambiará la economía de un ataque para inclinar la balanza a favor de los defensores.

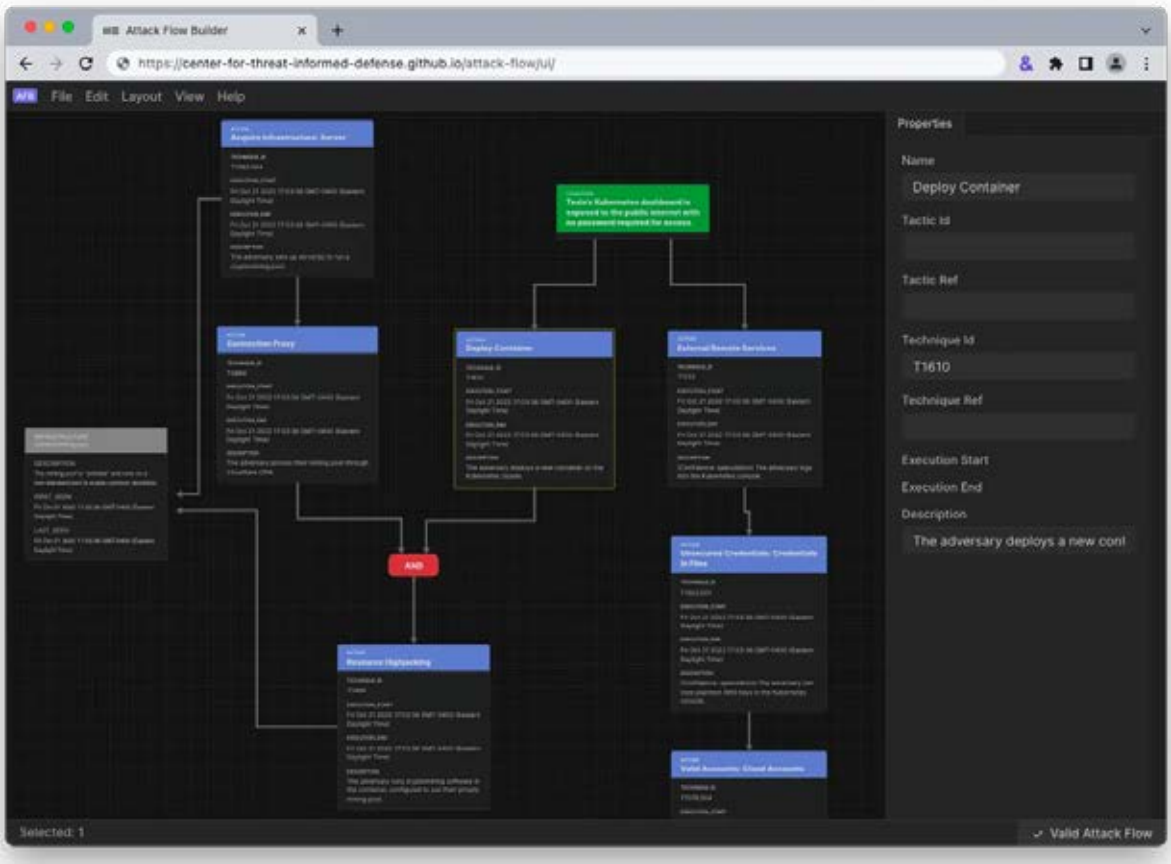


Figura 8: Desarrollador de flujo MITRE ATT&CK, flujo de ejemplo

Adicionalmente, estamos comenzando a incorporar estándares en nuestros informes, como el trabajo del controlador Wintapix que publican dos de nuestros investigadores.[26]

Refuerce sus tecnologías y procesos

No hay mejor momento que este para implementar tecnologías nuevas de seguridad o reevaluar su pila actual. Independientemente de las herramientas que elija, debe asegurarse de que puedan aprovechar la inteligencia artificial, el aprendizaje automático (ML), el aprendizaje profundo (DL) y el análisis avanzado. Estas funciones se volvieron esenciales para procesar el enorme volumen de datos que generan las organizaciones para identificar el tráfico riesgoso o anómalo que podría indicar una amenaza u otro riesgo.

Examinar y ajustar sus procesos actuales es imperativo, si quiere mantenerse por delante de sus adversarios. Esto incluye la redefinición de funciones y responsabilidades en su equipo de seguridad, la creación o actualización de los manuales de estrategias y hacer ejercicios de simulación para evaluar las competencias de su equipo o identificar brechas en los procesos que se deben tratar.

Muchas organizaciones actuales también están recurriendo a proveedores de confianza para que actúen como una extensión de su propio personal de seguridad. Nuestros servicios de seguridad basados en IA de FortiGuard comprenden una diversidad de herramientas poderosas, como los Next-Generation Firewall (NGFW); la telemetría y el análisis de redes; la EDR; la Detección y respuesta extendidas (XDR); la Protección contra riesgos digitales (DRP); Administración de información de seguridad y eventos (SIEM); el sandboxing en línea; el engaño; la orquestación, automatización y respuesta de seguridad (SOAR); y otras. Estas soluciones proporcionan a su organización funciones de detección y prevención de amenazas avanzadas que pueden ayudarlo a detectar y responder rápidamente a los incidentes de seguridad en toda la superficie de ataque.

Conclusión y perspectiva final

Esperamos que haya disfrutado la lectura de este informe tanto como nosotros disfrutamos creándolo. Sabemos que la ciberseguridad algunas veces puede parecer extremadamente compleja. Sin embargo, el campo está invariablemente poblado por personas entusiastas e inspiradas que trabajan incansablemente para proporcionar a la comunidad enfoques innovadores y optimizados para mejorar su postura de seguridad. La batalla contra el cibercrimen y las amenazas que plantean los Estados-Nación son un desafío constante, y como una industria, estamos completamente preparados para enfrentarlo y combatirlo.

El fortalecimiento de las asociaciones que comparten inteligencia frente a amenazas entre los sectores público y privado es crucial para combatir esta ciberguerra. La inteligencia frente a amenazas se debe poder procesar de inmediato mediante manuales de estrategias integrales, lo que puede ser un desafío sin estándares para compartir, herramientas e informes. No obstante, la inteligencia frente a amenazas compartida es un componente clave de cómo garantizamos respuestas eficaces, oportunas y sin fricciones. Creemos firmemente que los defensores actuales poseen un amplio acceso a herramientas, conocimientos y apoyo para comenzar a alterar la economía de un ataque, todo lo que representa una poderosa contramedida contra los adversarios.

[1] "MITRE ATT&CK Matrix for Enterprise", MITRE, 2015-2023.

[2] Douglas José Pereira dos Santos, "2H 2022 Global Threat Landscape Report: Key Insights for CISOs", Fortinet, 3 de marzo de 2023.

[3] "2H 2022 Global Threat Landscape Report", Fortinet, 3 de marzo de 2023.

[4] Geri Revay, "The Year of the Wiper", Fortinet, 24 de enero de 2023.

[5] Derek Manky, "The Latest Intel on Wipers", Fortinet, 23 de marzo de 2023.

[6] Douglas José Pereira dos Santos, "2H 2022 Global Threat Landscape Report: Key Insights for CISOs", Fortinet, 3 de marzo de 2023.

[7] "Exploit Prediction Scoring System", FIRST.org, 2015-2023.

[8] James Slaughter, Fred Gutierrez, and Shunichi Imano, "MOVEit Transfer Critical Vulnerability (CVE-2023-34362) Exploited as a 0-Day", Fortinet, 8 de junio de 2023.

[9] "Threat Signal Report: MOVEit Transfer Critical Vulnerability (CVE-2023-34362)", FortiGuard Labs, 2 de junio de 2023.

[10] "EPSS API," FIRST.org, 2015-2023.

[11] "Replication Through Removable Media", MITRE ATT&CK, 31 de mayo de 2017.

[12] "IPS Threat Encyclopedia: Raspberry.Robin.Worm", FortiGuard Labs, 14 de julio de 2022.

[13] "Increased Truebot Activity Infects U.S. and Canada-Based Networks", Cybersecurity and Infrastructure Security Agency, 6 de julio de 2023.

[14] "Exploitation for Client Execution", MITRE ATT&CK, 18 de abril de 2018.

[15] Fortinet Follina Blog Posts, consultado el 27 de julio de 2023.

[16] "Hijack Execution Flow: DLL Side-Loading", MITRE ATT&CK, 13 de marzo de 2020.

[17] FortiGuard Labs, "3CX Desktop App Compromised (CVE-2023-29059)", Fortinet, 30 de marzo de 2023.

[18] "Obfuscated Files or Information", MITRE ATT&CK, 31 de mayo de 2017.

[19] "Masquerading", MITRE ATT&CK, 31 de mayo de 2017.

[20] "Virtualization/Sandbox Evasion", MITRE ATT&CK, 17 de abril de 2019.

[21] "OS Credential Dumping", MITRE ATT&CK, 31 de mayo de 2017.

[22] "Input Capture", MITRE ATT&CK, 31 de mayo de 2017.

[23] "Process Injection", MITRE ATT&CK, 31 de mayo de 2017.

[24] Derek Manky, "Partnering to Disrupt Cybercrime", Fortinet, 14 de febrero de 2023.

[25] Douglas José Pereira dos Santos, "MITRE Attack Flow Gives CISOs Valuable Context for Better Risk Management", Fortinet, 3 de noviembre de 2022.

[26] Geri Revay and Hossein Jazi, "WINTAPIX: A New Kernel Driver Targeting Countries in the Middle East", Fortinet, 22 de mayo de 2023.

agosto 17, 2023 4:02 p. m.

2278529-0-0-ES