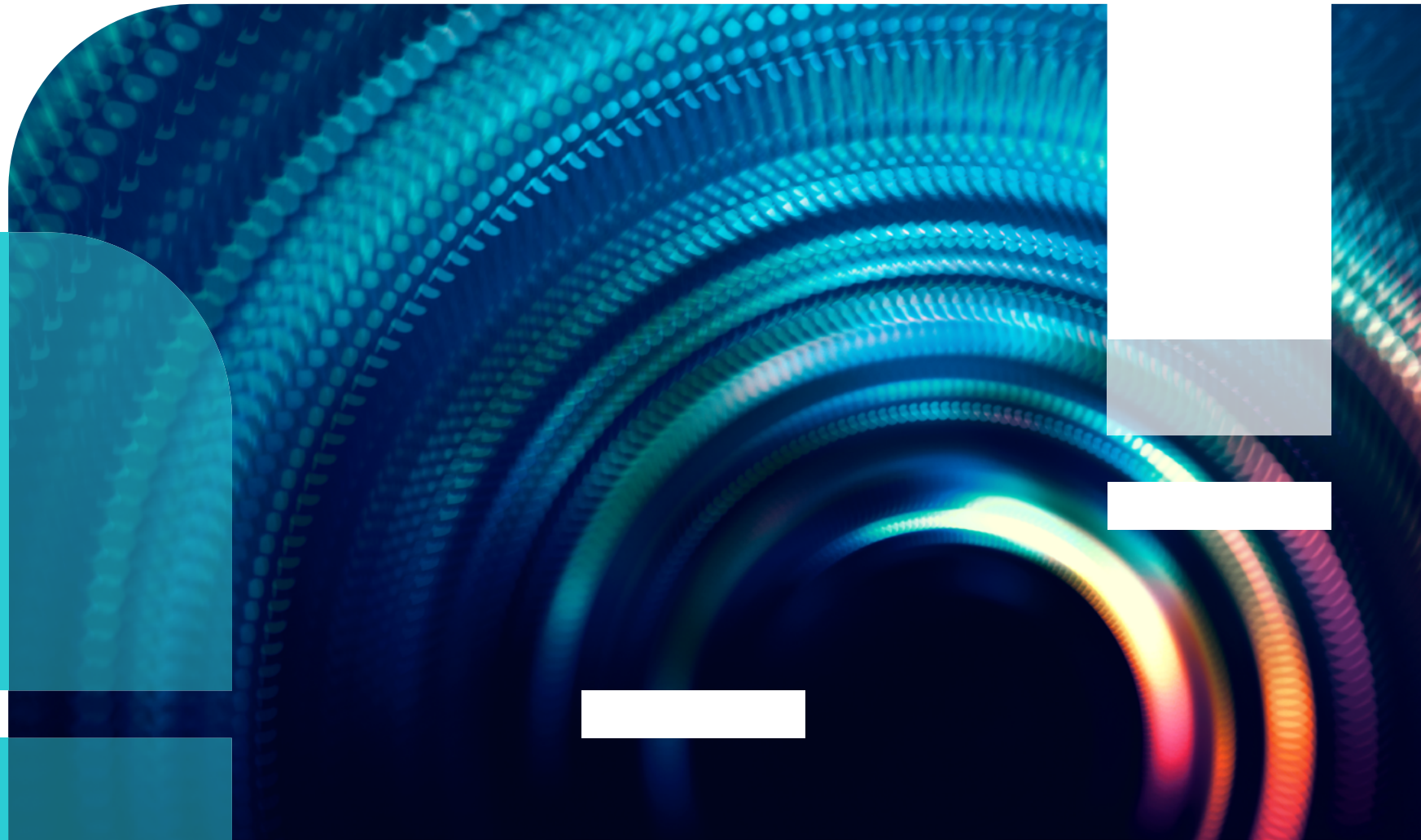
Segundo2H de 2023

Informe global del panorama de amenazas

Un informe semestral de FortiGuard Labs



Resumen ejecutivo

En el segundo semestre de 2023, el panorama de ciberseguridad observó una serie de desarrollos significativos que han afectado considerablemente la superficie de ataque digital. Entre estos se destaca el aumento de ciberataques sofisticados dirigidos a entidades de gran escala e infraestructura esencial.

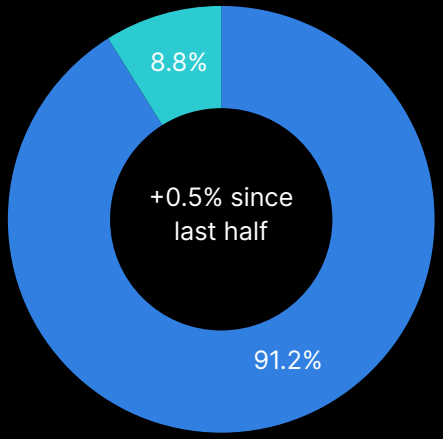
Si el creciente número de ataques no fuera suficiente para mantener a la mayoría de los CISO despiertos por la noche, el dominio de ciberseguridad se enfrenta simultáneamente al desafío continuo de atraer y retener profesionales calificados. La creciente demanda de expertos calificados en ciberseguridad, junto con la necesidad de que las organizaciones ofrezcan atractivas oportunidades de desarrollo profesional y entornos de trabajo, continúa destacando la importancia del capital humano para combatir las ciberamenazas.

La necesidad de comprender dónde se encuentran las brechas de su superficie de ataque en la detección, mitigación y respuesta es más vital que nunca y lo más impactante que podemos hacer es aclarar cómo el panorama de amenazas ha cambiado y cómo las organizaciones deben crear sistemas de redes seguros que puedan adaptarse rápidamente a las cambiantes demandas comerciales y al panorama de amenazas en evolución. Es por eso que publicamos este informe. Nuestro objetivo es ayudarlo a navegar por estos cambios y comprender dónde enfocar su tiempo y energía, utilizando sus recursos de la manera más impactante.

Los hallazgos de este informe representan la inteligencia colectiva de FortiGuard Labs, extraída de una amplia gama de sensores de red que recopilan eventos de amenazas cada día que se observan en entornos de producción en vivo en todo el mundo de más de 600K000 entornos y más de 10M de sensores que capturan cada detalle sobre amenazas que afectan nuestra tecnología de detección. Hemos examinado todos esos datos para encontrar y extraer información clave que esperamos ayude a guiarlo a través de los ciberdesafíos de 2024.

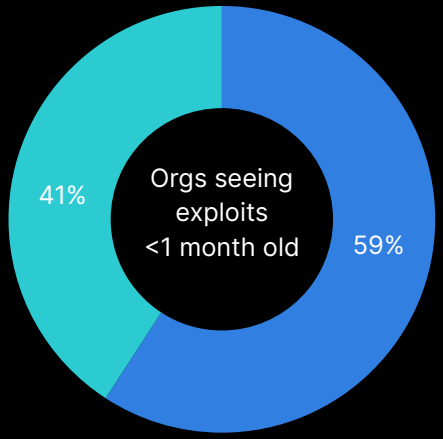
2H 2023 Active Threat Landscape at a Glance

Into the Red Zone



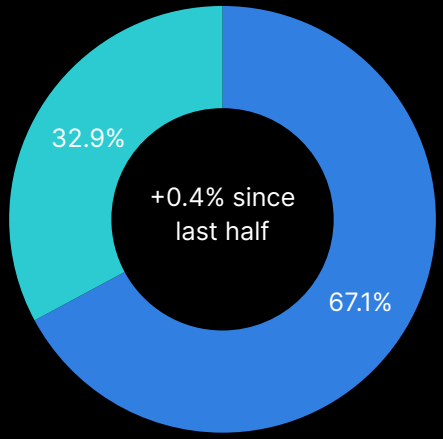
The percent of all endpoint vulnerabilities targeted by attacks remained steady, around 9%.

Exploit Dispersion



Attacks can spread quickly. 41% of organizations detected activity for exploits less than one month old.

ATT&CK Sightings



Sandbox and network detection and response (NDR) sensors observed activity for over two-thirds of MITRE ATT&CK techniques.

APT Groups

38/143

FortiRecon intelligence indicates 38 of the 143 advanced persistent threat (APT) groups listed by MITRE were active during this time.

Ransomware

40%+

More than 40% of ransomware and wipers targeted the industrial sector, indicating that cybercriminals are focused on OT and the supply chain.

Time-to-Exploitation

43%

On average, for new exploits identified, attacks occurred in 4.76 days after discovery. That's 43% faster than the prior period.

Una mirada a las tendencias de vulnerabilidades de seguridad, malware y botnet

FortiGuard Labs monitorea una amplia gama de sensores implementados globalmente que recopilan billones de eventos de amenazas en todo el mundo cada día. Este punto de vista único nos brinda una visión detallada y completa del panorama de las ciberamenazas, que incluye cómo cambian con el tiempo las tendencias de vulnerabilidades de seguridad, malware y botnets.

Exploits	Malware	Botnet
11,030 unique exploit detections, +10% over last half	39,896 unique variants detected, -11% from last half	319 unique botnets detected, -3% from last half
63 exploit detections per organization, +17% over last half	5,962 different active families, -16% from last half	4.3 active botnets per sensor, +/-0% from last half
73% of firms saw severe attacks, +4% over last half	16 families spread to more than 10% of organizations, -11% from last half	85 infection days in average, +2% over last half

Estos datos, descritos en la gráfica anterior, muestran que la creación y prevalencia de vulnerabilidades de seguridad están en aumento. Los cibercriminales están apuntando al número cada vez mayor de nuevas vulnerabilidades resultantes del crecimiento exponencial en el número y la variedad de dispositivos conectados y una explosión en nuevas aplicaciones y servicios en línea. Es natural que los ataques que buscan aprovechar esas vulnerabilidades también aumenten. Este aumento en el volumen de vulnerabilidades de seguridad por organización contribuye indudablemente a la prevalencia de los equipos de seguridad abrumados.

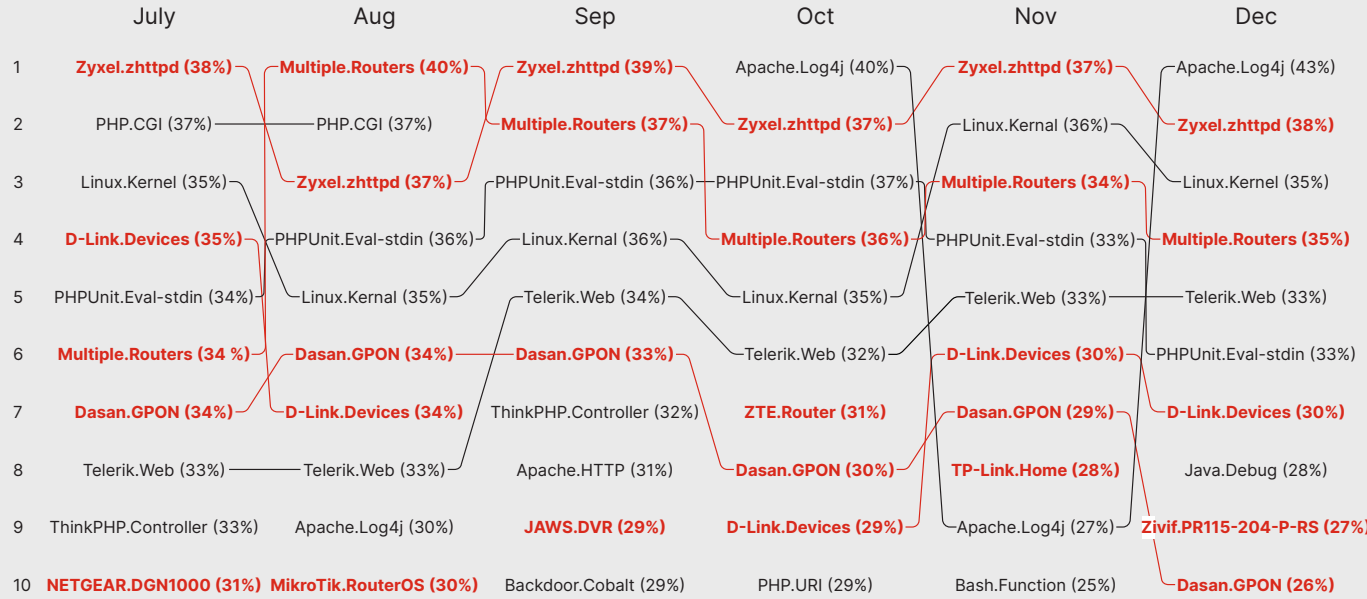
Curiosamente, después de aumentar durante el primer semestre de 2023, el volumen de muestras de malware que detectaron nuestros sensores disminuyó en el segundo semestre del año. Desafortunadamente para los defensores, esto no significa que el malware se esté saliendo de favor entre los atacantes inteligentes. La desaceleración observada probablemente se debe a que ciertos tipos de malware, en particular el ransomware, están adoptando un enfoque más dirigido, lo que conduce a un aumento del costo por incidente de ransomware. Esto también explica por qué el tráfico de bots se mantuvo estable durante este mismo tiempo.

Las vulnerabilidades de seguridad del IoT están en aumento

La actividad de explotación capturada por los sensores del Sistema de prevención de intrusiones (IPS) de FortiGuard que se ejecutan en nuestros Next-Generation Firewalls de FortiGate proporciona una visibilidad inigualable de cómo los actores de amenazas encuentran vulnerabilidades, explotan sus objetivos y construyen infraestructura maliciosa. Estos sensores a menudo son el primer punto de contacto con un adversario que busca exposiciones. Comencemos con una visión de las tecnologías que los atacantes sondean de manera más agresiva. No es de extrañar que los dispositivos del Internet de las cosas (IoT), que se muestran en rojo en la gráfica correspondiente, sean objetivos populares, en gran parte porque a menudo están protegidos o desprotegidos.

Si bien destacamos las alertas de brotes para los dispositivos del IoT aquí, nuestro equipo de FortiGuard Labs tuvo sus radares llenos de todo tipo de vulnerabilidades de seguridad adicionales en el 2H de 2023. Este es un resumen rápido de algunos de estos:

- Vulnerability[5]
- Vulnerabilidad de ejecución de código IBM Aspera Faspex[6]
- Attack[7]
- Attack[8]
- Vulnerability[9]
- Vulnerability[10]

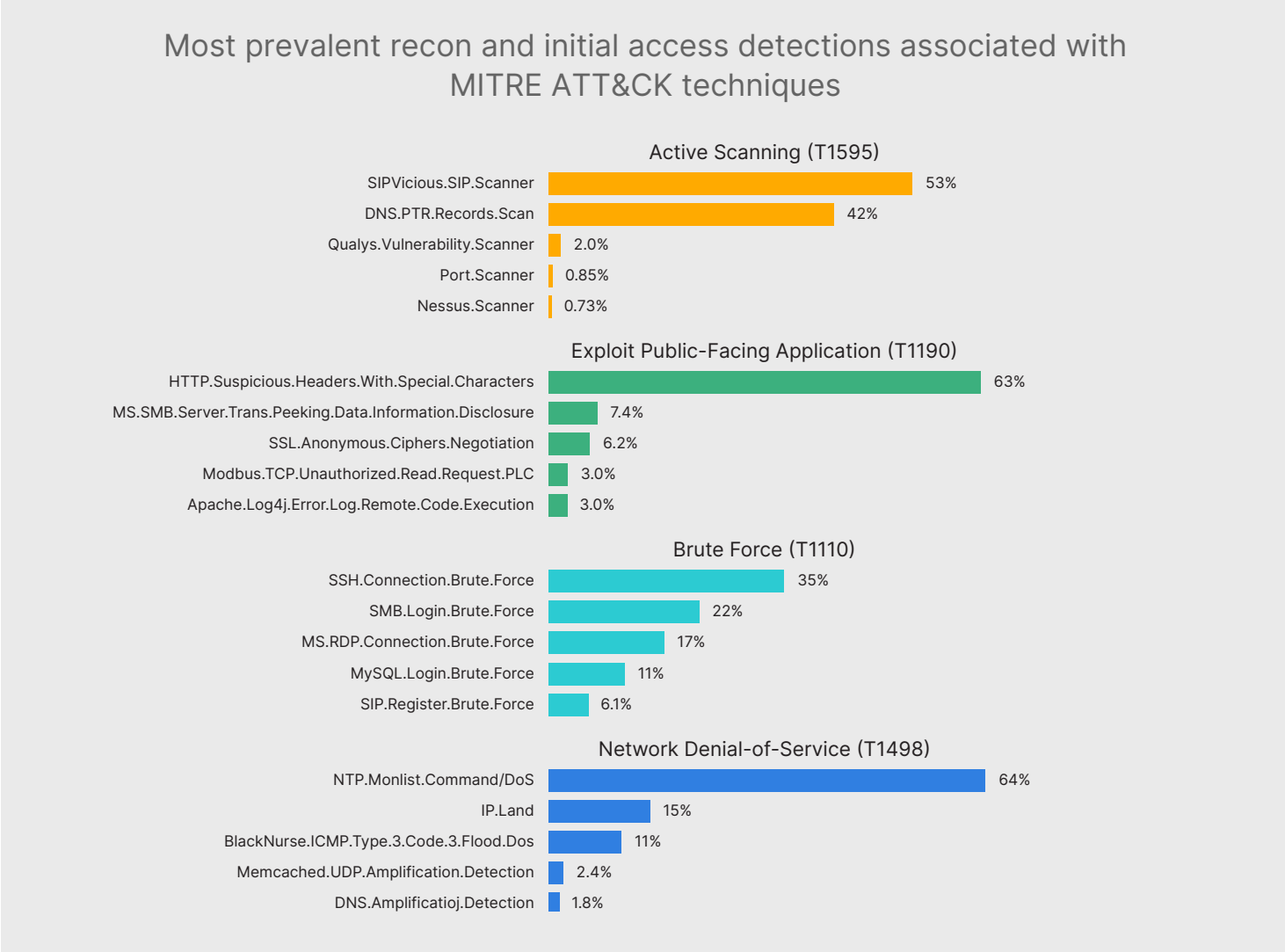


Las vulnerabilidades que afectan a enrutadores, cámaras y otros dispositivos del IoT fueron el foco de varias alertas de brotes publicadas por FortiGuard Labs durante 2023.[1]

El equipo de Zyxel Networks fue un objetivo favorito para las vulnerabilidades de seguridad durante la segunda mitad del año, con FortiGuard Labs emitiendo una alerta de brote sobre los firewalls de la empresa.[2] Quizás oliendo la sangre en el agua, los atacantes redescubrieron y aprovecharon una vulnerabilidad de Zyxel Networks relacionada con un enrutador de fin de vida, que se publicó inicialmente en 2017.[3]

Hablando de vulnerabilidades antiguas que atraen nueva atención, las vulnerabilidades de seguridad dirigidas a las cámaras web de Zivif (CVE-2017-17107) ocupó la lista de las 10 principales en diciembre de 2023. Estas vulnerabilidades de seguridad parecen estar relacionadas con los ataques continuos de Zerobot que alertamos a los profesionales de la seguridad a finales de 2022.[4] Este escenario muestra que las vulnerabilidades antiguas siempre se pueden hacer nuevas (y mejores) mediante actores de amenazas empresariales.

Cerramos esta revisión de vulnerabilidades de seguridad con otra gráfica que demuestra el amplio alcance de la actividad detectada por nuestros sensores IPS. A continuación, presentamos las cinco principales detecciones de vulnerabilidades de seguridad asociadas con cuatro técnicas clave MITRE ATT&CK [11] de exploración activa, vulnerabilidades de seguridad de aplicaciones públicas, fuerza bruta y DoS de red.



Los appliances de seguridad de red proporcionan inteligencia en el lado izquierdo del marco MITRE ATT&CK , lo que nos ayuda a comprender más sobre las amenazas que utilizan los actores maliciosos para intentar ingresar a las organizaciones. Idealmente, al aplicar el marco de trabajo de ATT&CK en su empresa, recomendamos recopilar fuentes de ATT&CK y crear un mapa de calor consolidado para usar en la búsqueda de amenazas, el trabajo en equipo púrpura, la emulación adversaria y la ingeniería de detección.

Seguimiento del movimiento entre familias de malware

Una vez que los actores de amenazas encuentran una vulnerabilidad explotable, su siguiente paso es a menudo implementar malware. Las muestras que recogen nuestras diversas soluciones antimalware ofrecen información sobre las herramientas populares de los adversarios para establecer un punto de apoyo, escalar privilegios, mantener la presencia y moverse lateralmente dentro de los entornos objetivo para alcanzar sus objetivos.

La figura de la siguiente página mide la proporción de organizaciones en cada región que detectaron variantes de las familias de malware más comunes durante el segundo semestre del año. El malware que gana un punto de apoyo en una región del mundo, como la familia JS/Agent, gana una tracción similar en la mayoría de las otras geografías.

Top malware families based on regional prevalence

	Africa	Asia	Europe	Latin America	Middle East	North America	Oceania
JS/Agent	40.9%	34.2%	34.0%	37.4%	30.9%	30.0%	35.9%
JS/Phishing	17.6%	15.9%	19.2%	19.8%	12.7%	12.0%	18.5%
MSIL/Kryptik	17.4%	22.6%	19.8%	16.6%	16.9%	4.8%	7.5%
HTML/Phish	16.5%	19.9%	18.6%	15.2%	13.9%	7.9%	12.0%
JS/ScrInject	20.1%	13.1%	11.9%	18.6%	33.4%	10.3%	18.7%
JS/Cryxos	12.8%	28.6%	13.6%	14.7%	12.1%	13.3%	18.7%
MSIL/GenKryptik	14.6%	20.8%	17.9%	16.1%	15.4%	4.3%	7.2%
PDF/Phishing	14.1%	12.8%	14.9%	12.9%	11.2%	8.9%	14.1%
MSIL/GenericKDS	11.8%	19.1%	15.2%	13.6%	12.7%	3.7%	6.1%
HTML/Phishing	12.5%	13.1%	12.0%	9.6%	9.2%	5.6%	7.3%
MSIL/Agent	11.6%	16.1%	14.6%	11.4%	12.1%	3.5%	5.6%
MSOffice/CVE_2018_0798	9.8%	15.0%	15.1%	9.4%	10.2%	3.4%	4.7%
JS/Redirector	13.7%	7.7%	9.6%	8.0%	7.8%	7.5%	10.7%
MSIL/Stealer	9.5%	14.6%	11.8%	10.3%	10.3%	2.8%	4.5%
NSIS/Injector	8.5%	13.4%	13.1%	7.1%	10.1%	2.4%	5.3%
MSOffice/CVE_2017_11882	8.4%	12.1%	11.0%	17.6%	9.5%	2.5%	3.4%
HTML/infObfus	11.8%	5.9%	6.3%	4.2%	10.1%	10.5%	15.7%
BAT/Agent	5.5%	9.1%	6.3%	9.0%	6.7%	3.7%	4.3%
W32/Injector	8.6%	11/9%	8.9%	6.8%	9.0%	2.2%	3.0%
MSExcel/CVE_2017_11882	8.2%	12/3%	8.6%	5.0%	7.4%	2.3%	3.3%

En caso de que desee volver a verificar sus análisis antivirus para detectar las variantes más comunes de JS/agente, estas son las tres principales que debe buscar, además de una variante final que aumentó rápidamente las clasificaciones de popularidad en el 2H de 2023:

- JS/Agent.CY!.tr[12]
- JS/Agent.F022!.tr[13]
- JS/Agent.PIV!.tr[14]
- JS/Agent.NDS!.tr[15]

Sin embargo, dos familias de malware han rebajeado la tendencia de uniformidad regional: JS/ScrInject y JS/Cryxos. Para el primero, la variante responsable es JS/ScrInject.B!.tr.[16] Este troyano de acceso remoto (RAT) ha estado circulando desde 2011 y tiene un ciclo de actividad semanal muy regular.[17] El otro es JS/Cryxos y, en particular, la variante JS/Cryxos.5478!.tr.[18] Este troyano, conocido por tener una variedad de capacidades subrepticias, parece estar impulsando la gran cantidad de detecciones en Asia.

Fuera de las familias genéricas más prevalentes que se muestran anteriormente, cuatro campañas de malware adicionales llamaron nuestra atención en el segundo semestre de 2023: AndroxGh0st, ransomware Apache ActiveMQ, Lazarus RAT y Agent Tesla. Cubrimos AndroxGh0st ampliamente en la sección de botnet, por lo que resumiremos los otros tres aquí.

Apache ActiveMQ

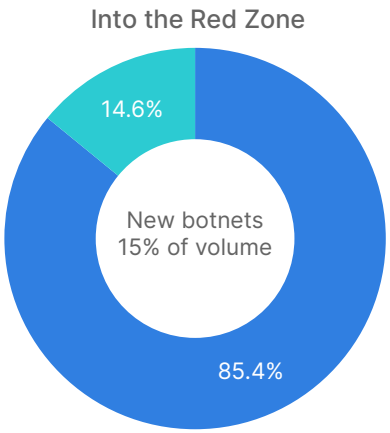
Apache ActiveMQ es un popular agente de mensajes de código abierto. Se divulgó una vulnerabilidad (CVE-2023-46604) en otoño de 2023 que permitió a un atacante remoto con acceso a la red de un agente ejecutar comandos shell arbitrarios manipulando tipos de clase serializados en el protocolo OpenWire.[19] Los informes surgieron en noviembre de que los atacantes aprovechaban esa falla en forma de ransomware HelloKitty.[20] FortiGuard Labs lanzó una alerta de brote que detallaba cómo los actores de amenazas aprovechaban esta falla al ejecutar campañas de ransomware dirigidas a servidores que ejecutaban versiones obsoletas y vulnerables de Apache ActiveMQ.[21]

RAT de Lazarus

Lazarus Group es un grupo de APT patrocinado por el gobierno norcoreano. En esta nueva campaña, se observó que Lazarus empleaba malware RAT basado en DLang en su entorno. El acceso inicial de Lazarus comienza con la explotación exitosa de CVE-2021-44228, la infame vulnerabilidad Log4j descubierta en 2021.[22]

Tesla del agente

FortiGuard Labs capturó una campaña de suplantación de identidad que propaga una nueva variante de Agent Tesla.[23] Esta conocida familia de malware utiliza un RAT basado en la red y un ladrón de datos para obtener acceso inicial al aprovechar las vulnerabilidades de Microsoft Office CVE-2017-11882 y CVE-2018-0802.[24] , [25] El módulo principal de Agent Tesla puede recopilar información confidencial del dispositivo de la víctima, como credenciales guardadas, información de registro de claves y capturas de pantalla del dispositivo.



Old versus new bots

Nuevos bots en el bloque: AndroxGh0st, Prometei y DarkGate

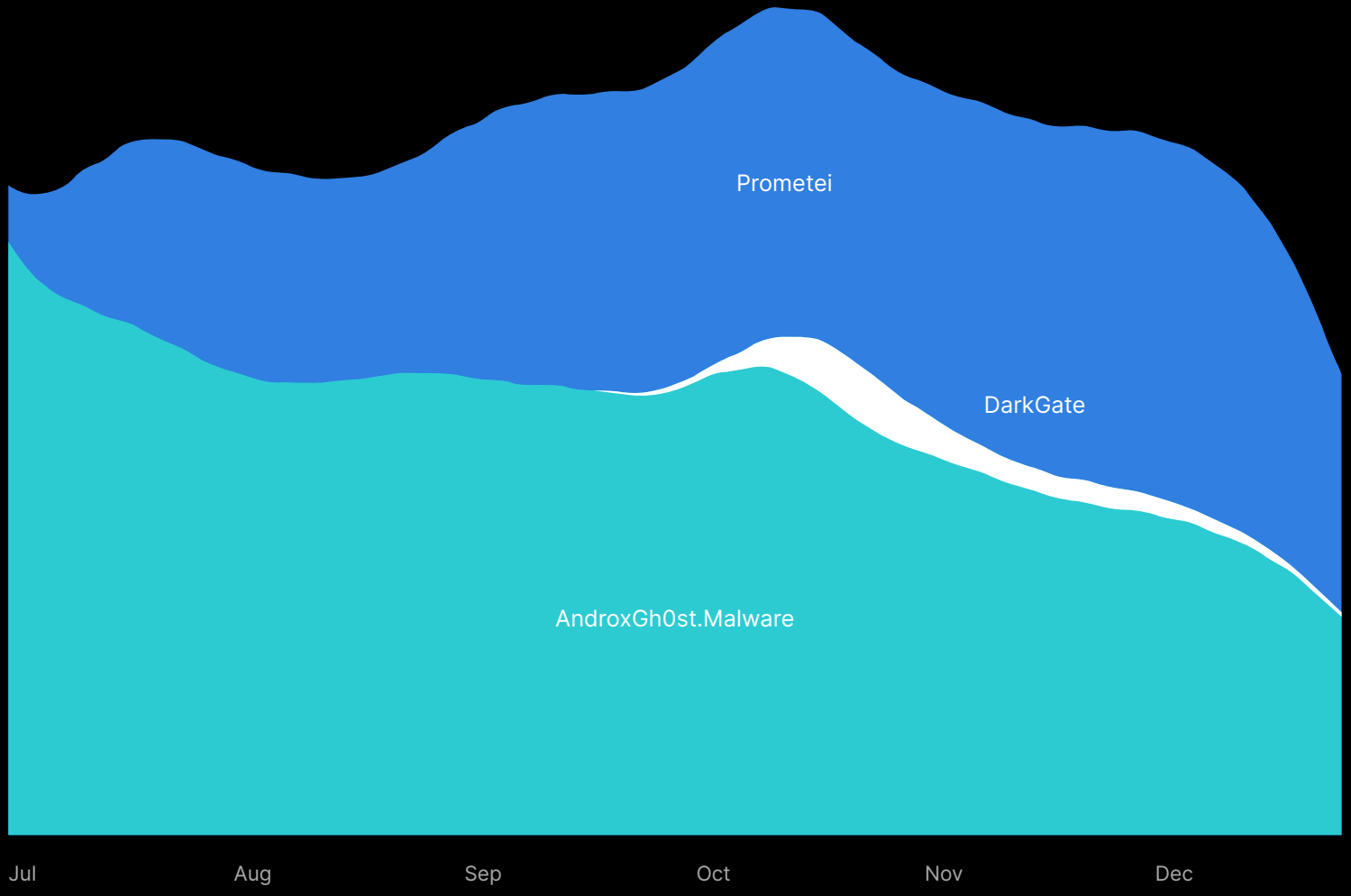
Una vez infectados con malware, los sistemas a menudo intentan comunicarse con hosts remotos para descargar cargas adicionales, establecer canales de comando y control (C2) y abrir puertas traseras en el entorno. Esto hace que el análisis del tráfico de botnets sea una parte importante del monitoreo del alcance completo de la actividad maliciosa.

Un gráfico de las botnets más activas inevitablemente se llena con muchas de las mismas que hemos visto durante años, incluyendo Gh0st ,Mirai y ZeroAccess. Esto demuestra dos cosas:

- Las botnets son resistentes. Se crean para persistir y, a pesar de los derribos coordinados de las fuerzas de seguridad, pueden ser difíciles de eliminar.
- La corrección de botnet es un proceso lento. Gran parte del tráfico de botnets que detectamos proviene de sistemas infectados que intentan comunicarse con botnets que ya no están activas.

Dicho esto, ocasionalmente surgen nuevas botnets que merecen atención. En el segundo semestre de 2023, tres nuevas botnets tomaron el centro de atención: AndroxGh0st, Prometei y DarkGate.

Volume of traffic associated with new botnets emerging in 2H 2023



AndroxGh0st

The AndroxGh0st botnet is related to the Python-based malware of the same name. It primarily targets user environment (.env) files, which often contain credentials for a variety of high-profile applications. AndroxGh0st includes numerous malicious functions to abuse Simple Mail Transfer Protocols (SMTP). It also scans and exploits exposed credentials and APIs and deploys web shells to maintain persistent access to systems.

We continue to observe widespread activity of AndroxGh0st malware in the wild exploiting multiple vulnerabilities. It specifically targets the PHPUnit (CVE-2017-9841), Laravel Framework (CVE-2018-15133), and Apache Web Server (CVE-2021-41773) vulnerabilities to spread and conduct information-gathering attacks on the target networks.[26, 27, 28] Fortinet was credited with exposing telemetry on AndroxGh0st, showing over 40,000 devices infected by the botnet.[29]

Prometei

Prometei is malware that can remotely control infected machines. It's capable of spreading laterally across networks, stealing password credentials, executing arbitrary commands, and downloading and executing additional malicious components. Prometei can also perform cryptocurrency mining and has self-updating capabilities.

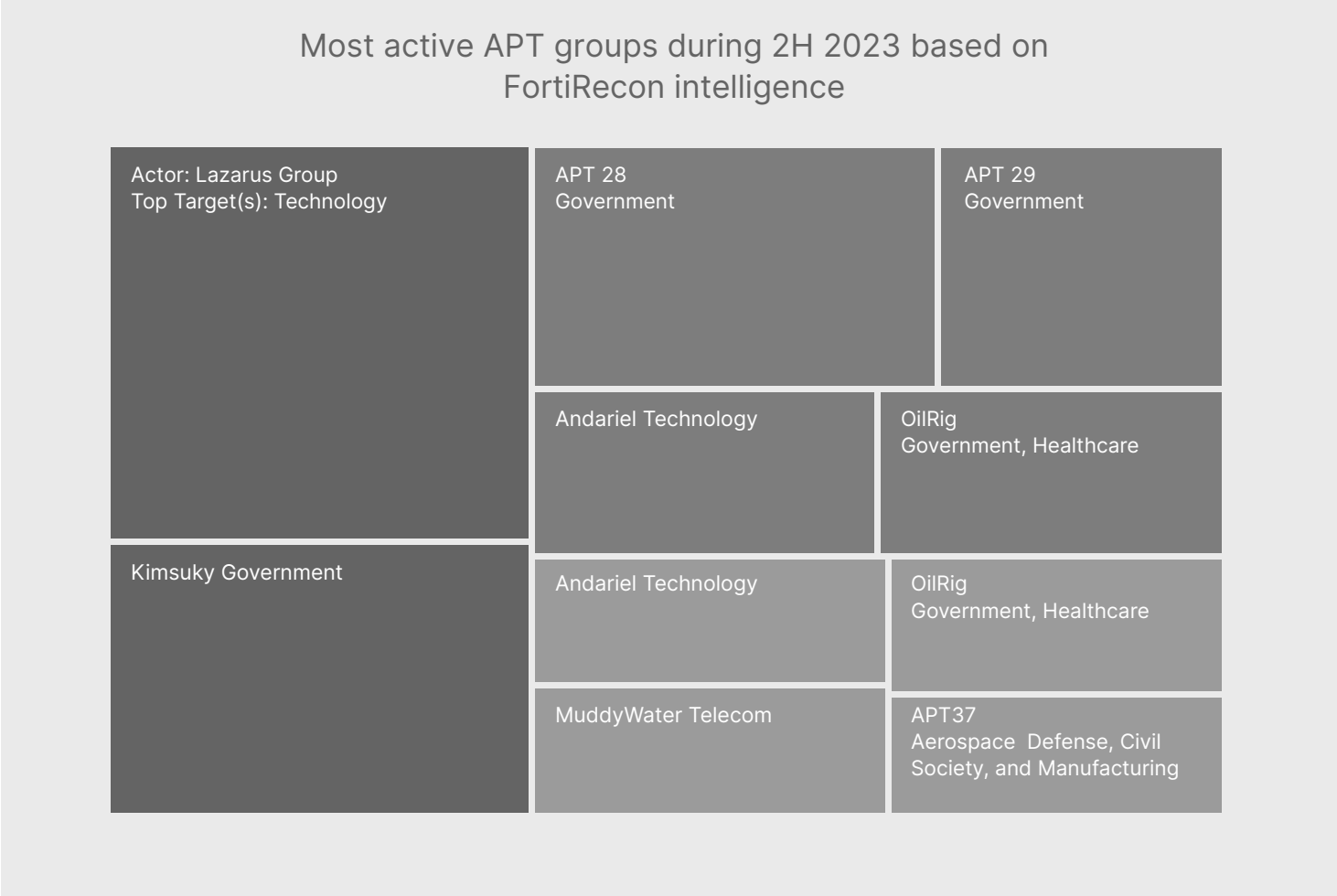
This malware strain was recently reinvented, and we created new IPS signatures to aid in detection.[30] This retooling worked well, as the Prometei botnet has subsequently been catapulted to the sixth spot on our list for total traffic volume across our sensors in 2H 2023.

DarkGate

Though it's a distant third to AndroxGh0st and Prometei, the DarkGate botnet warrants mention. The DarkGate malware, which has a range of capabilities from remote access to cryptomining to information stealing, was first reported in 2017. Since then, its creators have used it only for specific campaigns. But in mid-2023, the purported author offered to sell it, and the malware soon began making wider rounds.[31] We saw the DarkGate botnet emerge after the Qakbot takedown as a possible successor.[32] Whether DarkGate has a future as a leading tool for cybercriminals remains to be seen.

APT más activas

En la primera mitad del año, observamos una actividad significativa entre los grupos de APT y ese volumen se mantuvo estable durante el resto de 2023. Los grupos de APT continúan siendo altamente adaptables a los cambios en el panorama digital y son cada vez más sigilosos a medida que planifican y ejecutan cuidadosamente los ataques. La siguiente imagen ofrece una mirada a los grupos de APT más activos durante la segunda mitad del año.



Los hallazgos más recientes de los investigadores indican un cambio definitivo en las tácticas del grupo de APT de Corea del Norte, Lazarus. Durante el último año y medio, revelaron tres RAT diferentes creadas utilizando tecnologías poco comunes durante el desarrollo, como QtFramework, PowerBasic y DLang. Esto indica que Lazarus Group es una organización madura y capaz, que generalmente utiliza vulnerabilidades de seguridad de N-Day y técnicas conocidas para violar a las empresas del sector tecnológico, como intercambios de cadenas de bloqueo y empresas de desarrollo de software. Los ataques del grupo han sido bastante lucrativos, con una compensación de más de USD 100 millones solo en robos de criptomonedas.

Otro grupo que estuvo activo en estos últimos meses de 2023 fue APT 28, utilizando vulnerabilidades de N-Day en Outlook y Winrar para robar credenciales de New Technology Lan Manager (NTLM), centrándose en violar organizaciones gubernamentales, así como empresas en las industrias de educación superior, fabricación y aeroespacial. El grupo se dirigió a organizaciones en Europa del Este, con múltiples campañas dirigidas a interrumpir las operaciones y robar información de estas empresas. Este mismo grupo también utilizó días cero no divulgados anteriormente este año para continuar con el ciberespionaje y robar datos. APT 28 también se ha alejado del uso de puertas traseras y compromete dispositivos periféricos en la red y ahora utiliza servicios legítimos como Google Drive y Microsoft OneDrive para exfiltrar datos sensibles.

Penetrando en la zona roja

Priorizar las vulnerabilidades para su corrección es más importante que nunca, dado que la tasa de descubrimiento y divulgación continúa acelerándose. Según la publicación de este informe, hay más de 222,000 vulnerabilidades en la lista de vulnerabilidades y exposiciones comunes (Common Vulnerabilities and Exposures, CVE).[33] Fuimos testigos de un nuevo récord en 2023, con un total de 30,000 nuevas vulnerabilidades publicadas, un aumento del 17 % con respecto al año anterior.

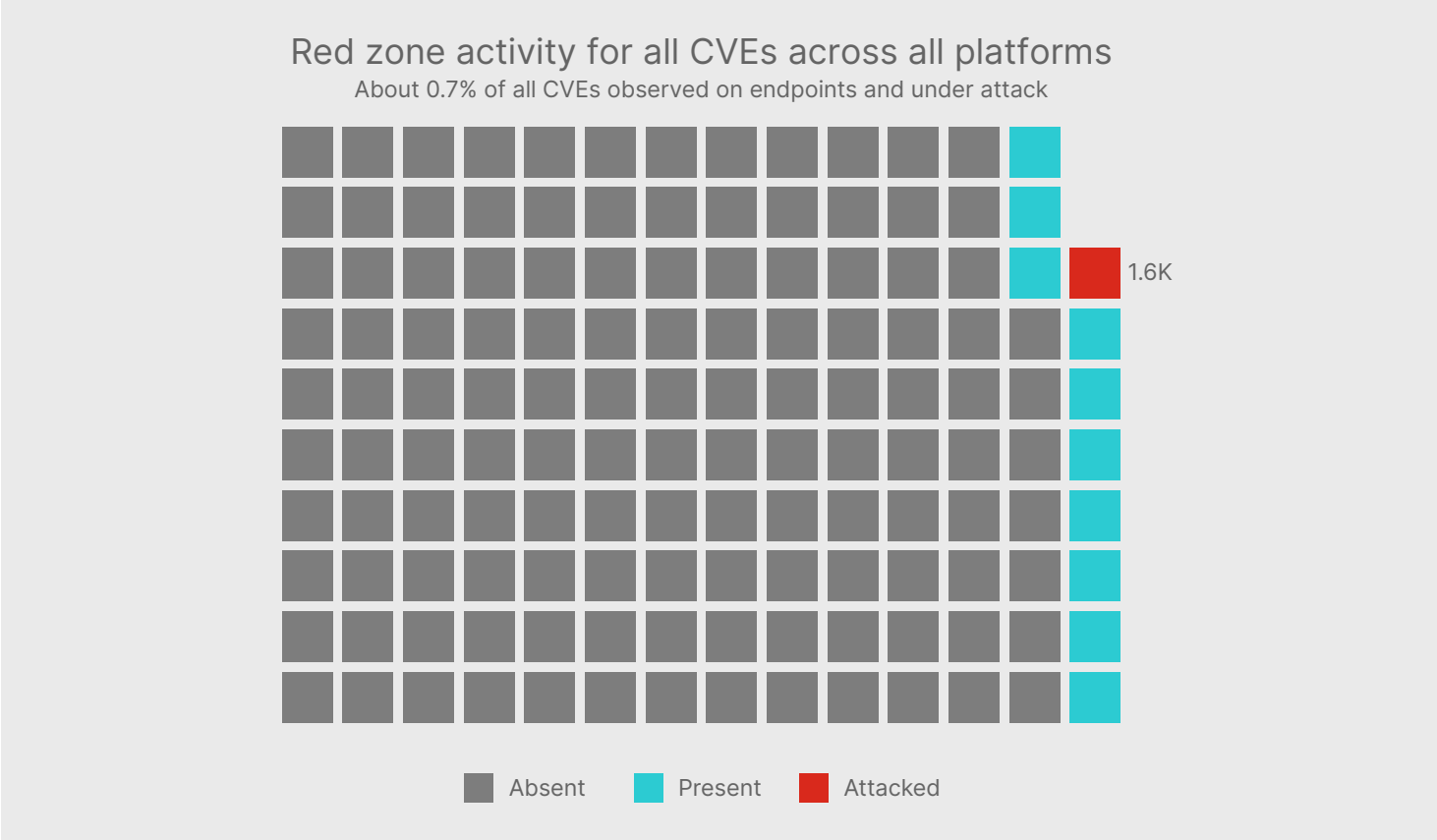
En 2022, presentamos el concepto de “zona roja”, que ayuda a los lectores a comprender mejor qué tan probable (o improbable) es que los actores de amenazas aprovechen una vulnerabilidad específica.[34] Esto permite a los equipos de seguridad enfocarse en las vulnerabilidades que presentan el mayor riesgo al priorizar los esfuerzos de corrección. Afortunadamente, nuestros datos muestran que un pequeño subconjunto (12.5 %) de todas las CVE históricas están presentes y no se corrigen en los endpoints en entornos activos. Esto se representa en la relación de cuadrados azules frente a grises en la gráfica adyacente.

Además, solo una fracción (<1 %) de todas las vulnerabilidades se explotaron en el 2H de 2023. Esa proporción se ha mantenido notablemente estable con el tiempo, lo que es una buena noticia para los equipos de seguridad.

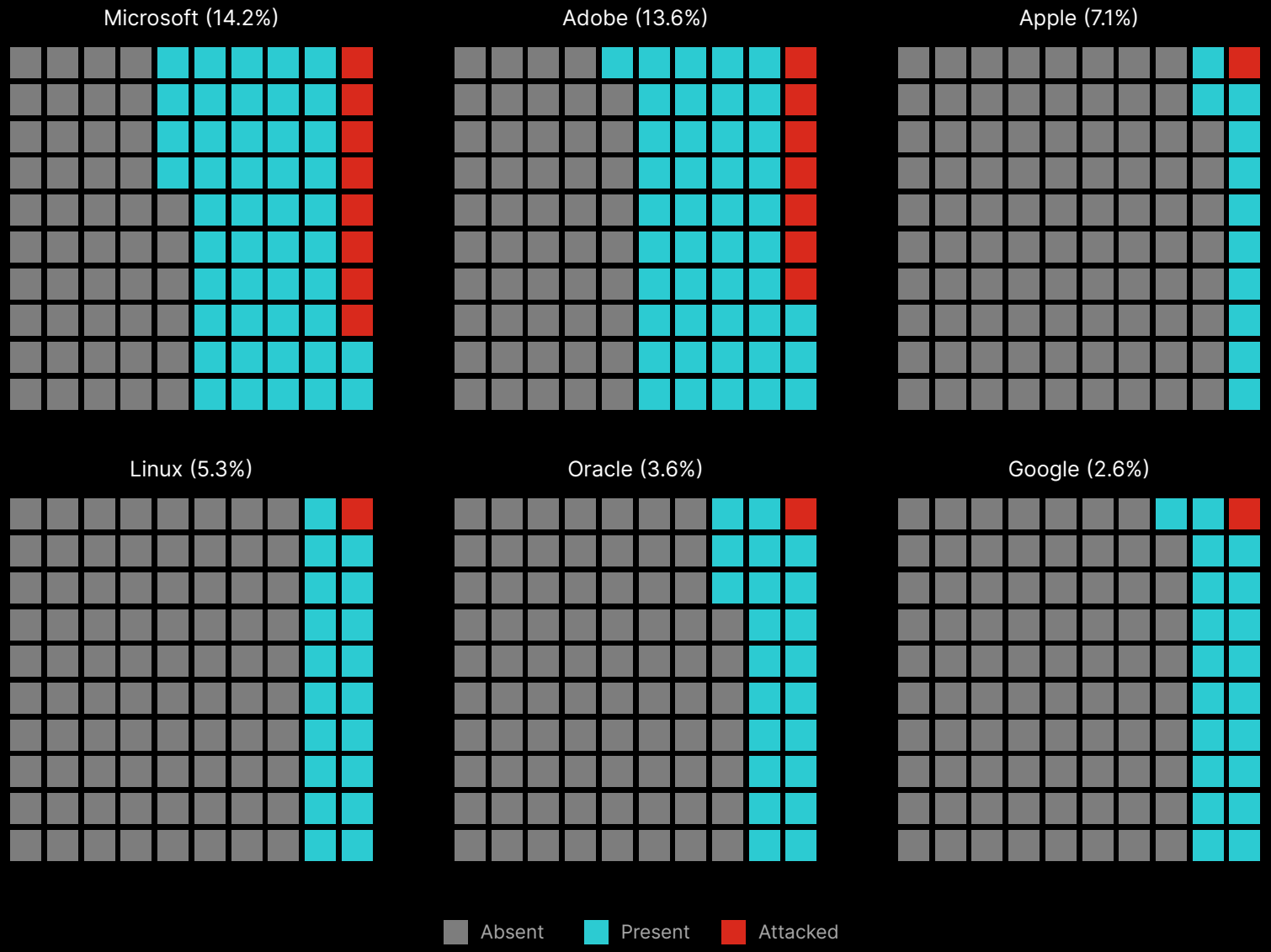
30K

nuevas vulnerabilidades en todas las industrias se publicaron en 2023, lo que marca un aumento del 17 % con respecto al año anterior.

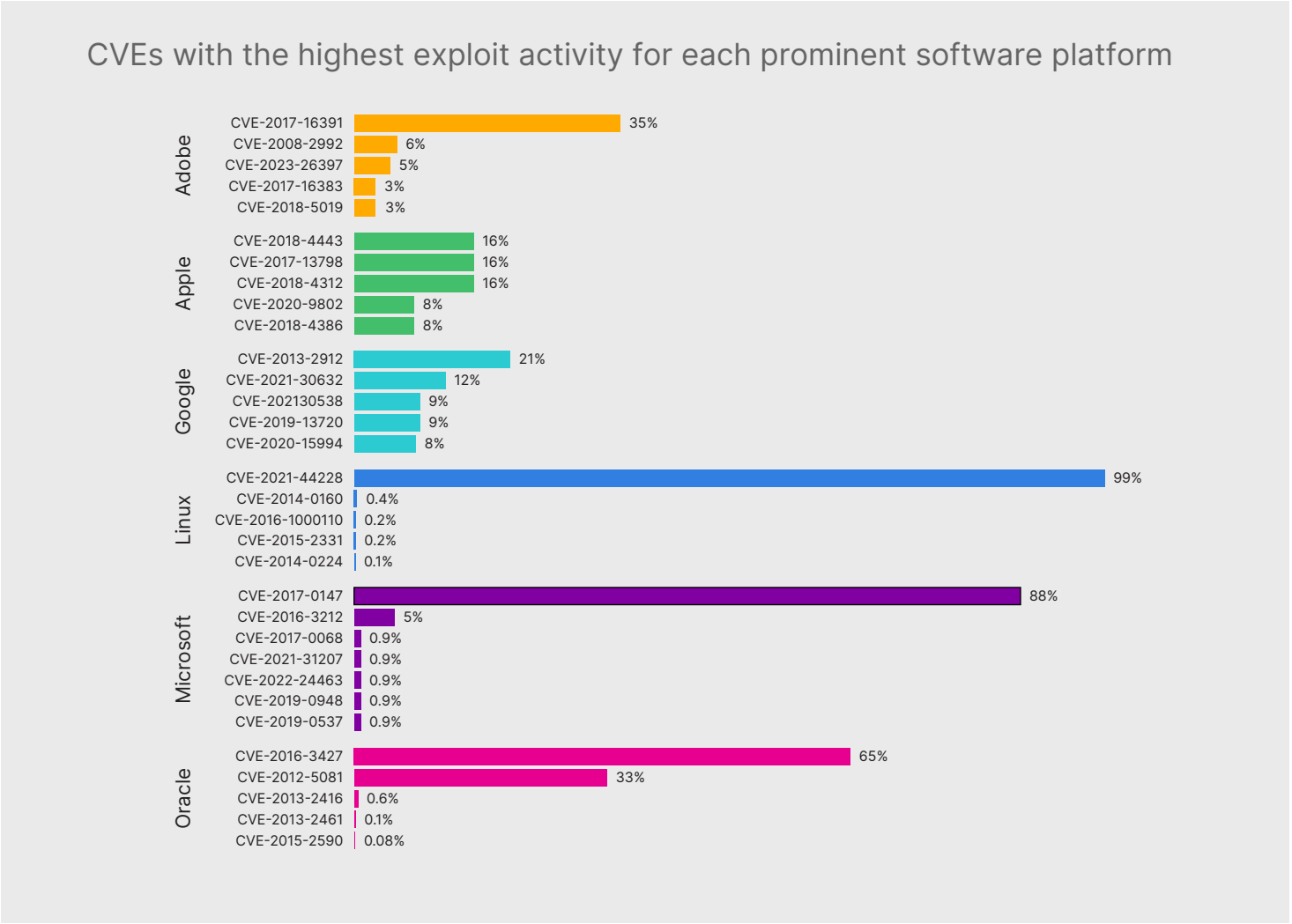
Por supuesto, la zona roja para muchas plataformas de software destacadas es sustancialmente mayor. Por ejemplo, la superficie de ataque de Microsoft es 20 veces mayor que el promedio general (14 %) y el doble que la de Apple (7 %) y Linux (5 %). En términos prácticos, cuanto mayor sea la zona roja, más esfuerzo y se requerirán parches automatizados para la corrección oportuna de vulnerabilidades de alto riesgo con vulnerabilidades de seguridad activas.



Red zone activity for CVEs affecting prominent platforms



A continuación, presentamos las cinco principales vulnerabilidades que componen la zona roja de cada plataforma en función de la prevalencia de intentos de exploit detectados:



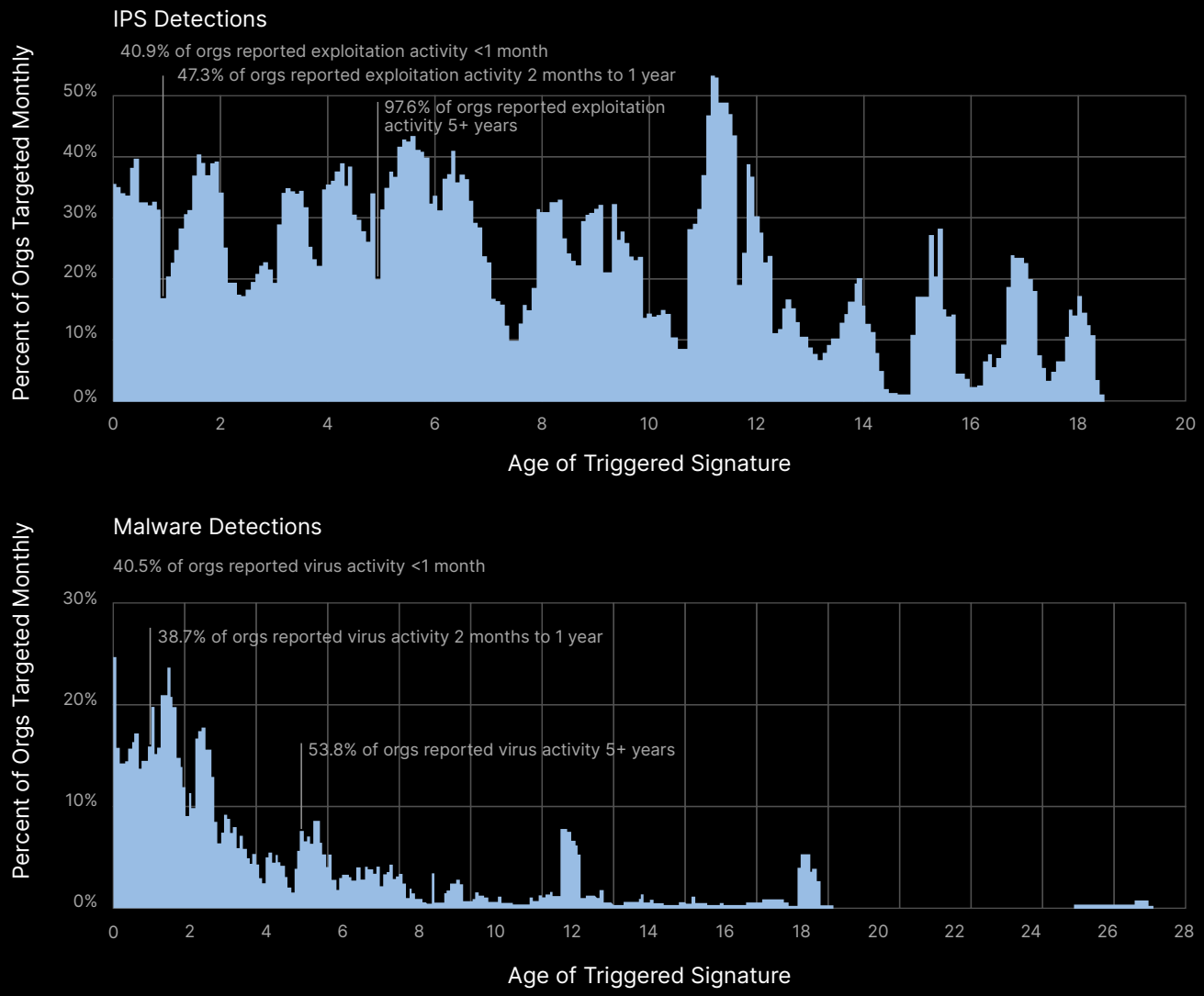
La participación de la actividad de la zona roja en las vulnerabilidades difiere drásticamente entre las plataformas. Un 99 % completo de la zona roja de Linux está dominada por vulnerabilidades de seguridad dirigidas a CVE-2021-44228.35 Compare eso con Apple, donde las tres principales vulnerabilidades representan aproximadamente el 16% de la actividad de vulnerabilidades de seguridad.

La mayoría de estas vulnerabilidades de la zona roja no son nuevas. Solo dos se publicaron en 2023 y solo uno de ellos surgió en la segunda mitad del año (CVE-2023-44487).[36] El resto abarca la última década. Además, tenga en cuenta que las vulnerabilidades de seguridad "antiguas" no se ralentizan: la principal vulnerabilidad para la mitad de las plataformas enumeradas se descubrió al menos cinco años antes.

De la predicción de vulnerabilidades de seguridad al brote

Como hemos discutido anteriormente, cuando se trata de vulnerabilidades, lo antiguo sigue siendo nuevo para muchos atacantes. Para comprender la prevalencia de esta tendencia, identificamos todas las vulnerabilidades de seguridad y muestras de malware que ocurrieron en el 2H de 2023 junto con la proporción de organizaciones que registraron detecciones. Luego trazamos esas firmas de acuerdo con el momento en que se crearon y agregaron a los dispositivos de Fortinet. Los gráficos de la siguiente página miden la vida útil activa de las amenazas de exploit y malware.

Age and prevalence of exploits and malware detected in 2H 2023

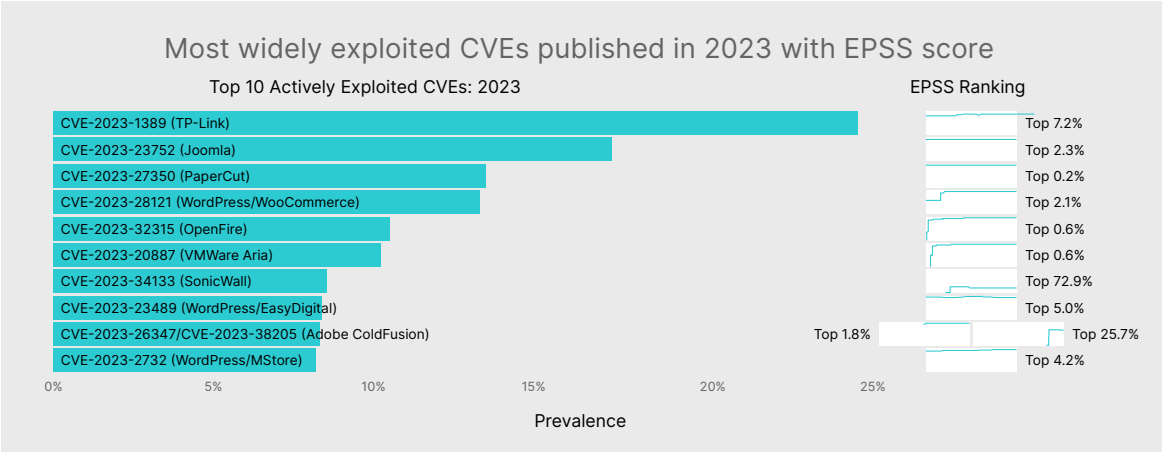


Seguimos observando actores de amenazas que explotan vulnerabilidades de más de 15 años. Casi todas las organizaciones (98 %) han detectado vulnerabilidades de seguridad que han existido durante al menos cinco años. Sin embargo, hay mucho espacio para que las nuevas amenazas lleguen a la escena: el 41 % de las organizaciones también detectaron vulnerabilidades de seguridad de firmas de menos de un mes de antigüedad. Sin embargo, con respecto al malware, poco más de la mitad de las organizaciones han detectado variantes que han existido durante cinco años o más, mucho menos de lo que vemos para las vulnerabilidades de seguridad.

Este análisis genera algunas perspectivas críticas sobre el panorama de las ciberamenazas. Las vulnerabilidades de seguridad y el malware tienen velocidades y alcances muy similares relacionados con su propagación, pero la longevidad de cada uno difiere. Las variantes de malware desaparecen más rápidamente a medida que el nuevo código reemplaza al viejo. Las vulnerabilidades de seguridad muestran una vida activa mucho más larga porque las vulnerabilidades a las que se dirigen los cibercriminales pueden permanecer sin parches durante años.

En términos prácticos, esto refuerza la importancia de estar atento a la higiene de la seguridad, ya que es probable que los atacantes no dejen de aprovechar las vulnerabilidades más antiguas. También es un gran recordatorio para que los profesionales de la seguridad actúen rápidamente a través de un programa consistente de parcheo y actualización cuando surgen nuevas vulnerabilidades que probablemente se exploten.

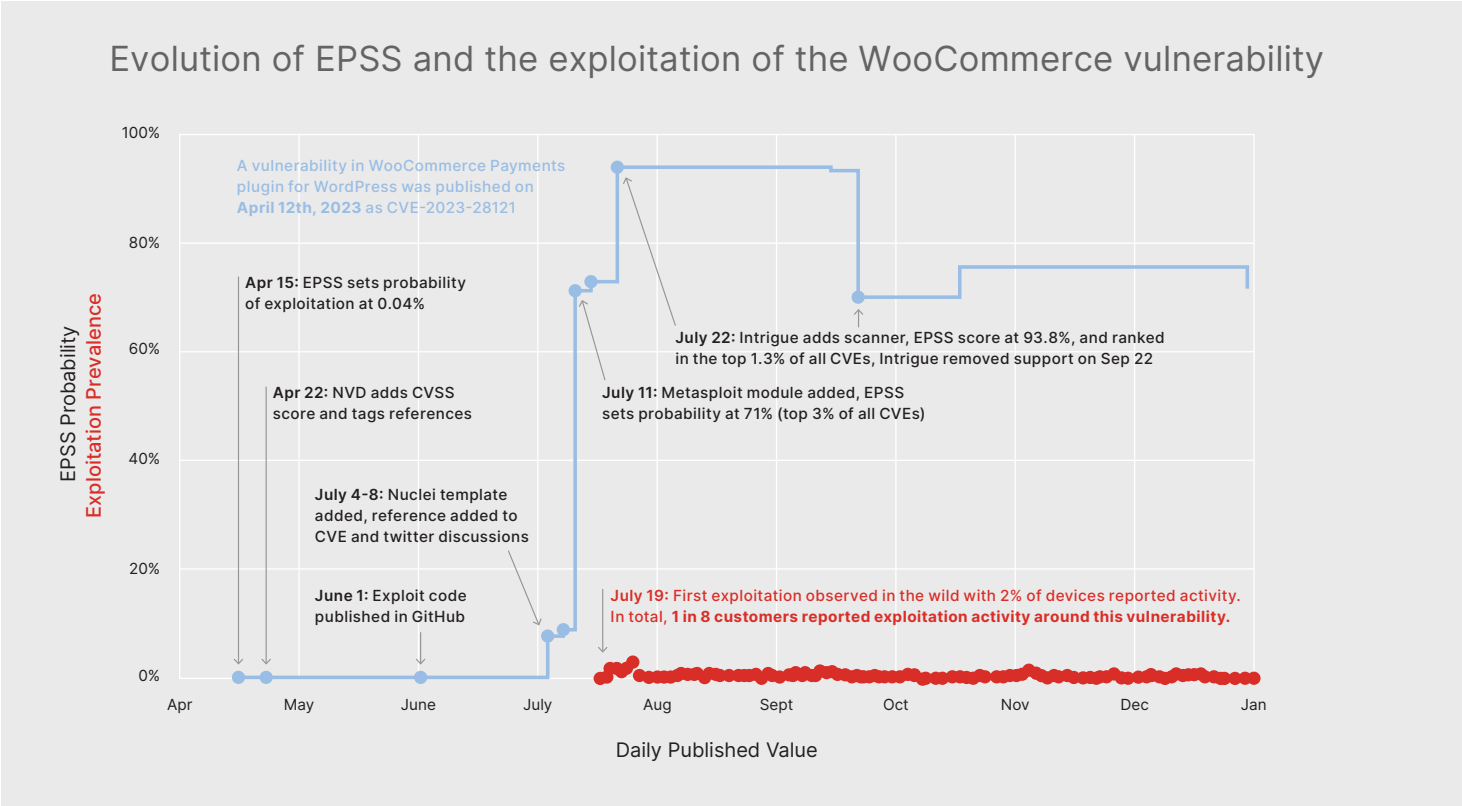
¿Cómo puede rastrear las vulnerabilidades emergentes que tienen más probabilidades de ser atacadas? El Sistema de puntuación de predicción de vulnerabilidades de seguridad (EPSS) existe para este propósito exacto.[37] Fortinet es uno de los principales contribuyentes a los datos de vulnerabilidades de seguridad que impulsan el EPSS. El siguiente gráfico muestra las vulnerabilidades publicadas en 202 que fueron las más atacadas por la actividad de vulnerabilidades de seguridad en la segunda mitad del año.



98%

de las organizaciones han detectado vulnerabilidades de seguridad que han existido durante al menos cinco años.

Veamos más de cerca qué tan preciso es el EPSS para identificar vulnerabilidades que probablemente se aprovechen. La gráfica a continuación destaca la puntuación del EPSS para la vulnerabilidad que afecta el complemento WooCommerce Payments para WordPress (CVE-2023-28121).[38] Esta CVE se publicó el 12 de abril de 2023 y EPSS la evaluó inicialmente como de baja probabilidad de vulnerabilidades de seguridad. Esa evaluación se revisó drásticamente después de que se lanzara una plantilla de Nuclei y un módulo Metasploit a principios de julio. Dados estos cambios, la vulnerabilidad aumentó al 3 % superior de los puntajes del EPSS con una probabilidad del 71 % de aprovechar las vulnerabilidades de seguridad en los próximos 30 días.

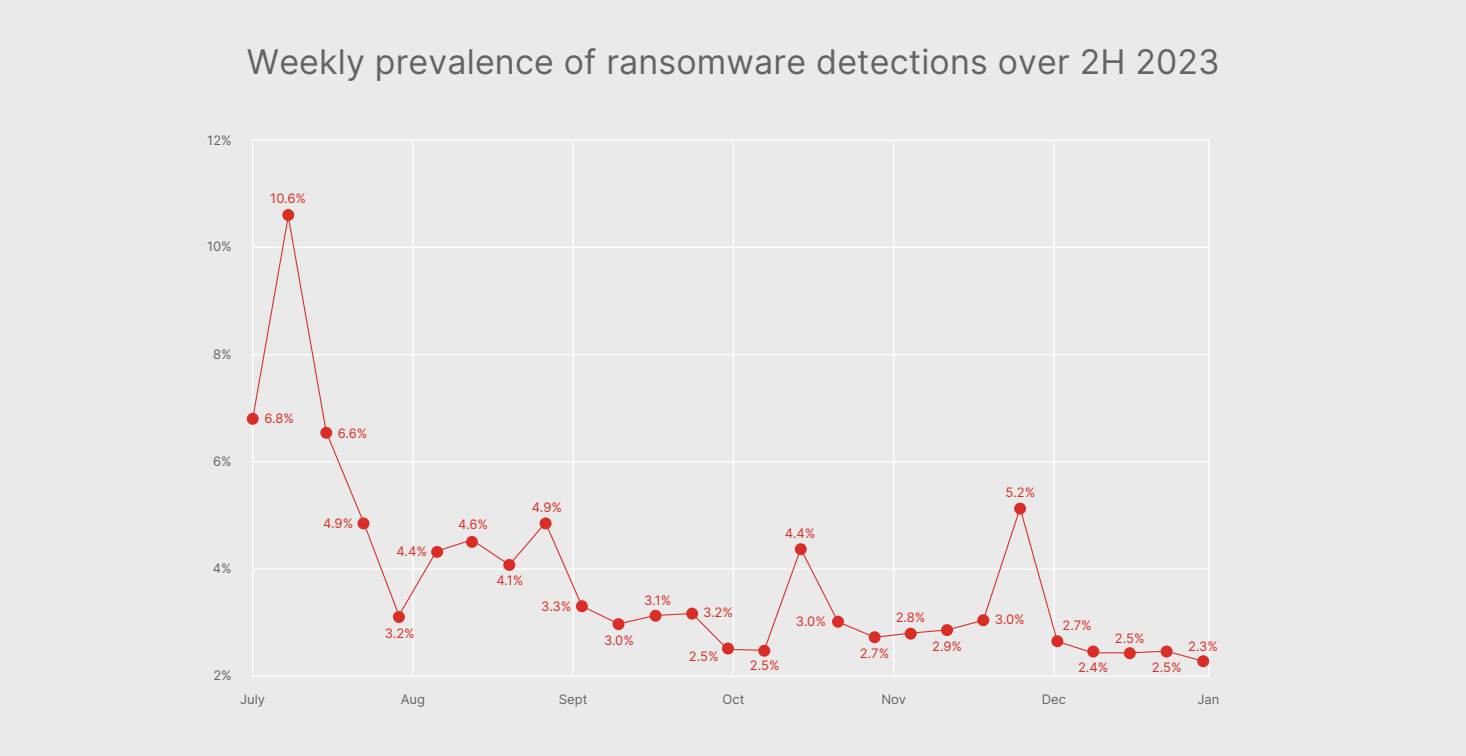


Poco después de esta revisión del EPSS, nuestro equipo observó los primeros signos de vulnerabilidad de seguridad en su entorno el 19 de julio. En este caso, el EPSS proporcionó un sistema eficaz de alerta temprana antes del brote de ataques, lo que dio a los defensores una ventaja valiosa en la corrección.

Con la reducción significativa del tiempo de explotación en un 43 % a solo 4.76 días, la presión sobre los recursos de ciberdefensa ya ampliados se ha intensificado. La capacidad de examinar rápidamente una lista priorizada de vulnerabilidades, administrando eficazmente estas "bombas de tiempo de tamizaje", ahora es más crítica que nunca. Integrar esta priorización en su proceso de administración de parches le proporciona una estrategia clara y urgente para la mitigación de riesgos, mejorando su postura de ciberseguridad en un panorama de amenazas en rápida evolución.

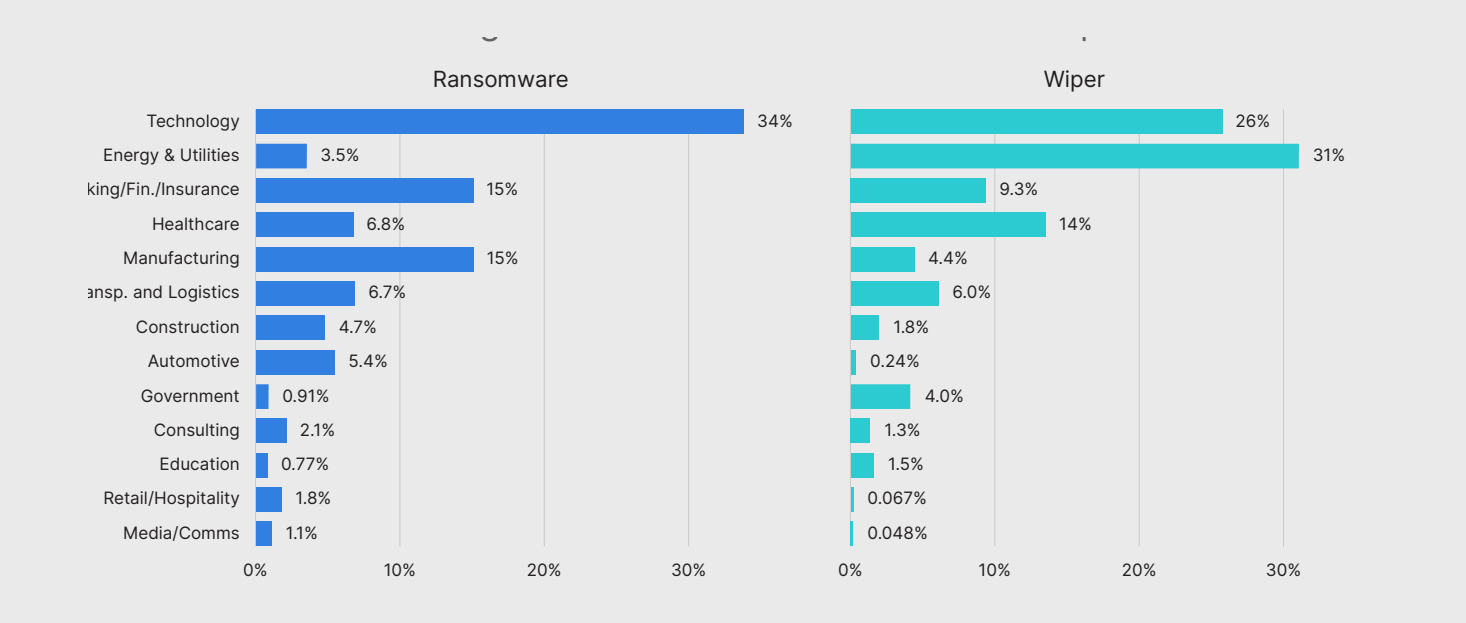
Los ataques de ransomware se dirigen cada vez más a industrias críticas

El ransomware continúa manteniendo a los equipos de seguridad activos por la noche. Según una encuesta reciente de Fortinet, más del 80 % de los líderes están "muy" o "extremadamente" preocupados por el ransomware.[39] En nuestros sensores, las detecciones de ransomware aumentaron 13 veces más en el primer semestre de 2023. A eso le siguió una caída del 70 % durante la segunda mitad del año, durante la cual también vimos menos organizaciones que detectaron variantes de ransomware.



Muchos de estos altibajos se remontan a la dinámica de las pandillas de ransomware. Algunos siguen una estrategia de alto volumen y bajo margen, lo que da como resultado un mayor número de variantes y víctimas de ransomware. Otras pandillas se enfocan en menos organizaciones que pueden pagar rescates más grandes mediante ataques altamente dirigidos.

En nuestro informe de predicciones de amenazas de 2024, pronosticamos que los adversarios que buscan pagos más grandes dirigirían su atención a industrias críticas como la atención médica, los servicios públicos, la fabricación y las finanzas. Como se predijo, en el 2H de 2023, presenciamos un cambio de la estrategia tradicional de "rociar y rezar", con cibercriminales que adoptan un enfoque más dirigido combinado con demandas de rescate que se disparan.[40]



La gráfica anterior proporciona un desglose de la industria de todas las muestras de ransomware y wiper que recogieron nuestros sensores durante la segunda mitad de 2023. La presencia significativa de industrias como la energía, la atención médica, la fabricación, el transporte y la logística, y la automotriz ofrece alguna evidencia de que nuestra predicción toma forma. En total, los sectores industriales experimentaron el 44 % de todas las detecciones de ransomware y wiper para el 2H de 2023. Esta tendencia es preocupante por muchas razones, especialmente porque las violaciones críticas de la industria pueden tener un impacto considerable y adverso en la sociedad.

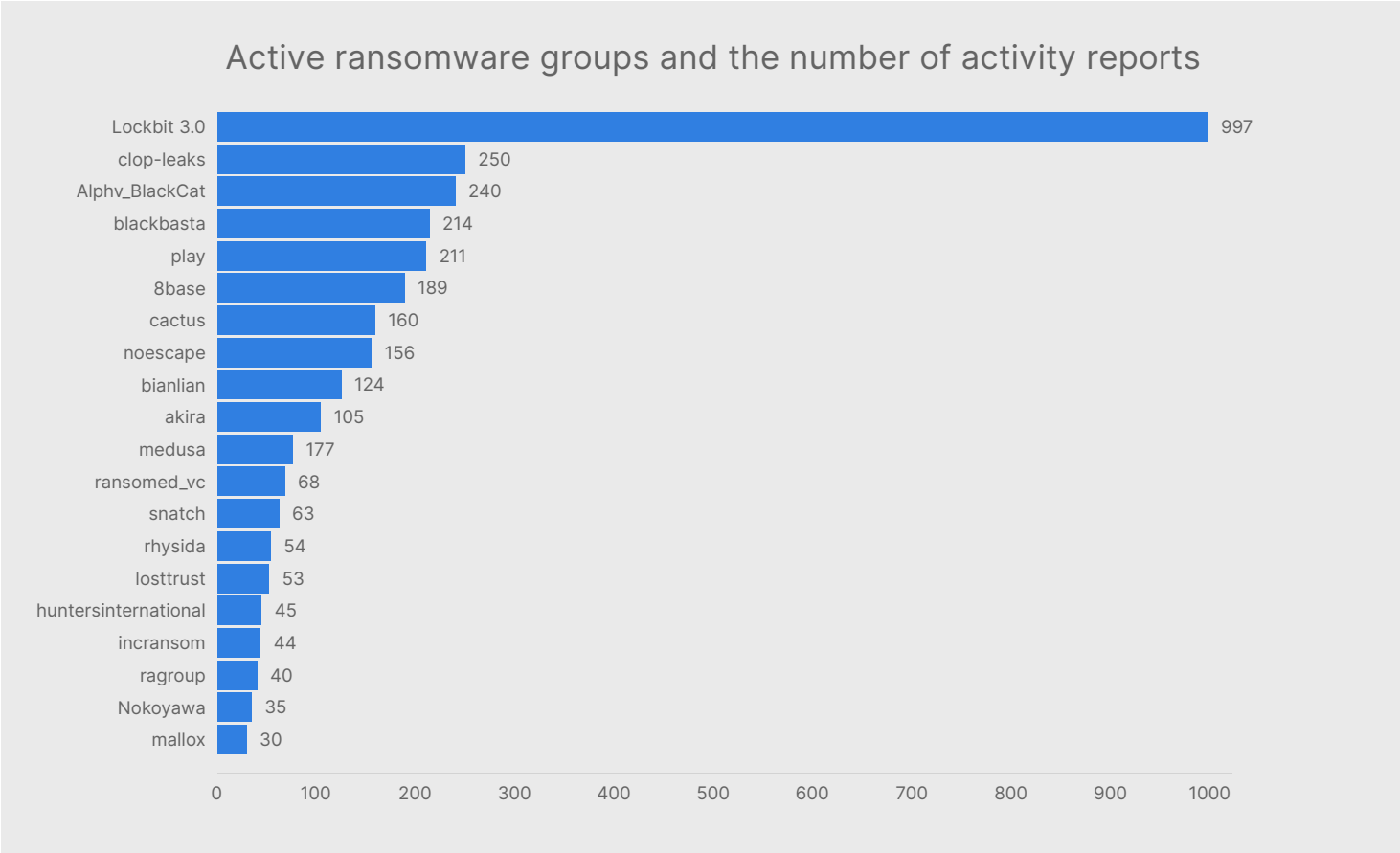
44%

de las organizaciones industriales experimentaron casi la mitad de todas las detecciones de ransomware y wiper en el segundo semestre de 2023.

Grupos de ransomware

En la última mitad del año, los actores de amenazas anunciaron 23 nuevas cepas de malware, ocho cepas de malware móviles, 15 ofertas de malware como servicio (MaaS) y seis nuevos programas de ransomware como servicio (RaaS).

Un ejemplo notable de un nuevo grupo de ransomware que surgió a finales de 2023 es Ransomed.VC, que inicialmente sirvió como foro, pero luego se transformó en un sitio de filtración de datos centrado en ransomware. Las acciones del grupo Ransomed.VC sirven como testimonio de las tácticas dinámicas empleadas por los grupos de ransomware actuales. Su participación en asuntos geopolíticos, alianzas con otros grupos, participación en violaciones de datos y promoción de servicios DDoS los ha establecido rápidamente como uno de los principales actores en el cambiante ámbito del cibercrimen.



El grupo hacktivista GhostSec también anunció un nuevo ransomware llamado GhostLocker en la web oscura. Este anuncio representa la expansión del grupo en el ámbito de la prestación de servicios de ransomware, destacando la naturaleza en constante evolución del panorama de amenazas y la aparición de nuevas herramientas dentro de la comunidad del cibercrimen. Los miembros de GhostSec utilizan principalmente Telegram y X para compartir sus listas de objetivos y resultados de ataques, lo que demuestra cómo el monitoreo de la web oscura puede servir como un sistema de advertencia temprana para nuevas iniciativas de cibercrimen. En cuanto al foro de cibercrimen en idioma ruso conocido como XSS, un actor de amenazas que utilizaba el seudónimo "malwareguy" promovió activamente una herramienta de creación diseñada para el ransomware de caos versión 4.0. La presencia de dichas ofertas en foros clandestinos es otro ejemplo de las amenazas en curso y en evolución que plantean los cibercriminales, así como la necesidad de monitorear la web oscura en busca de discusiones que puedan darnos una visión de los posibles vectores de ataque futuros. Esperamos que esta tendencia se intensifique a medida que avancemos en 2024.

Mapa de calor global de ATT&CK

MITRE ATT&CK es un repositorio ampliamente utilizado de tácticas, técnicas y procedimientos adversarios (TTP).41 Ofrece un lenguaje común desarrollado a partir de observaciones del mundo real que utilizan las organizaciones y los equipos de ciberseguridad para crear modelos de amenazas y defensas basadas en amenazas. Muchas soluciones de Fortinet ofrecen visibilidad de los TTP de ATT&CK y presentamos dos de ellas en esta sección.

La primera fuente de descubrimiento de técnicas ATT&CK es a través de nuestras soluciones de sandboxing. Millones de sensores en todo el mundo recopilan archivos sospechosos que se envían a través de una serie de motores antivirus, análisis conductual, análisis estático y dinámico, IA y ML, e inteligencia para identificar comportamientos sutiles indicativos de su amenaza subyacente. Los TTP identificados a través de este método se interpretan mejor como capacidades que posee el malware en su entorno durante el 2H de 2023.

La imagen de la página siguiente muestra las técnicas más prevalentes bajo cada táctica. Los porcentajes corresponden a la proporción de organizaciones que observaron malware con capacidades correspondientes a cada TTP.

Top ATT&CK techniques observed via sandbox solutions

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Replication Through Removable Media: 48%	Exploitation for Client Execution: 27%	Hijack Execution Flow: 33%	Process Injection: 34%	Obfuscated Files/Info: 20%	Input Capture: 43%	System info Discovery: 21%	Replication Through Removable Media: 60%	Data from Local System: 25%	Application Layer Protocol: 44%	Exfiltration Over Alternative Protocol: 96%	System Shutdown/ Reboot: 69%
Phishing: 31%	WMI: 22%	Boot/Logon Autostart Execution: 30%	Hijack Execution Flow: 22%	Masquerading: 15%	OS Credential Dumping: 37%	File and Directory Discovery: 1 5%	Taint Shared Content: 28%	Input Capture: 25%	Ingress Tool Transfer: 20%	Automated Exfiltration: 3%	Data Encrypted for Impact: 15%
Valid Accounts: 9%	Command and Scripting Interpreter: 19%	Create/Modify System Process: 15%	Boot/Logon Autostart Execution: 20%	Virtualiz./ Sandbox Evasion: 15%	Unsecured Credentials: 15%	Virtualiz./ Sandbox Evasion: 11%	Use Alternate Authentication Material: 4%	Email Collection: 17%	Non-Application Layer Protocol: 18%	Exfiltration Over C2 Channel: 0.4%	Inhibit System Recovery: 5%
Drive-by Compromise: 8%	Shared Modules: 14%	Scheduled Task/Job: 14%	Create/Modify System Process: 10%	Impair Defenses: 11%	Steal Web Session Cookie: 3%	Process Discovery: 11%	Software Deployment Tools: 3%	Automated Collection: 13%	Encrypted Channel: 11%		Service Stop: 4%
Exploit Public-Facing Application: 3%	Scheduled Task/Job: 8%	Office Application Startup: 5%	Scheduled Task/Job: 9%	Process Injection: 10%	Credentials from Password Stores: 0.8%	Software Discovery: 11%	Remote Services: 3%	Browser Session Hijacking: 6%	Non-Standard Port: 6%		Data Destruction: 3%
	Native API: 5%	Event Triggered Execution: 1.0%	Access Token Manipulation: 4%	Hijack Execution Flow: 7%	Network Sniffing: 0.2%	Query Registry: 8%	Exploitation of Remote Services: 0.7%	Clipboard Data: 6%	Proxy: 0.8%		Resource Hijacking: 1%
	System Services: 3%	Browser Extensions 0.6%%	Event Triggered Execution: 1.0%	Modify Registry: 5%	Forge Web Credentials: 0.004%	Remote System Discovery: 8%	Lateral Tool Transfer: 0.7%	Archive Collected Data: 3%	Web Service: 0.5%		Endpoint Denial of Service: 1%
	Inter-Process Comm.: 0.8%	Valid Accounts: 0.3%	Abuse Elevation Control Mechanism: 0.3%	Hide Artifacts: 5%		Application Window Discovery: 6%		Video Capture: 2%	Data Encoding: 0.07%		Data Manipulation: 0.6%
	User Execution: 0.2%	Pre-OS Boot: 0.3%	Valid Accounts: 0.2%	Indicator Removal on Host: 3%		System Network Configuration Discovery: 6%		Screen Capture: 2%	Remote Access Software: 0.05%		Defacement: 0.4%
	Software Deployment Tools: 0.06%	Boot/Logon Initialization Scripts: 0.2%	Boot/Logon Initialization Scripts: 0.1%	Deobfuscate/ Decode Files/Info: 3%		Network Service Discovery: 1%		Data from Info Repositories: 0.5%	Data Obfuscation: 0.04%		Firmware Corruption: 0.2%

Falling — Rising

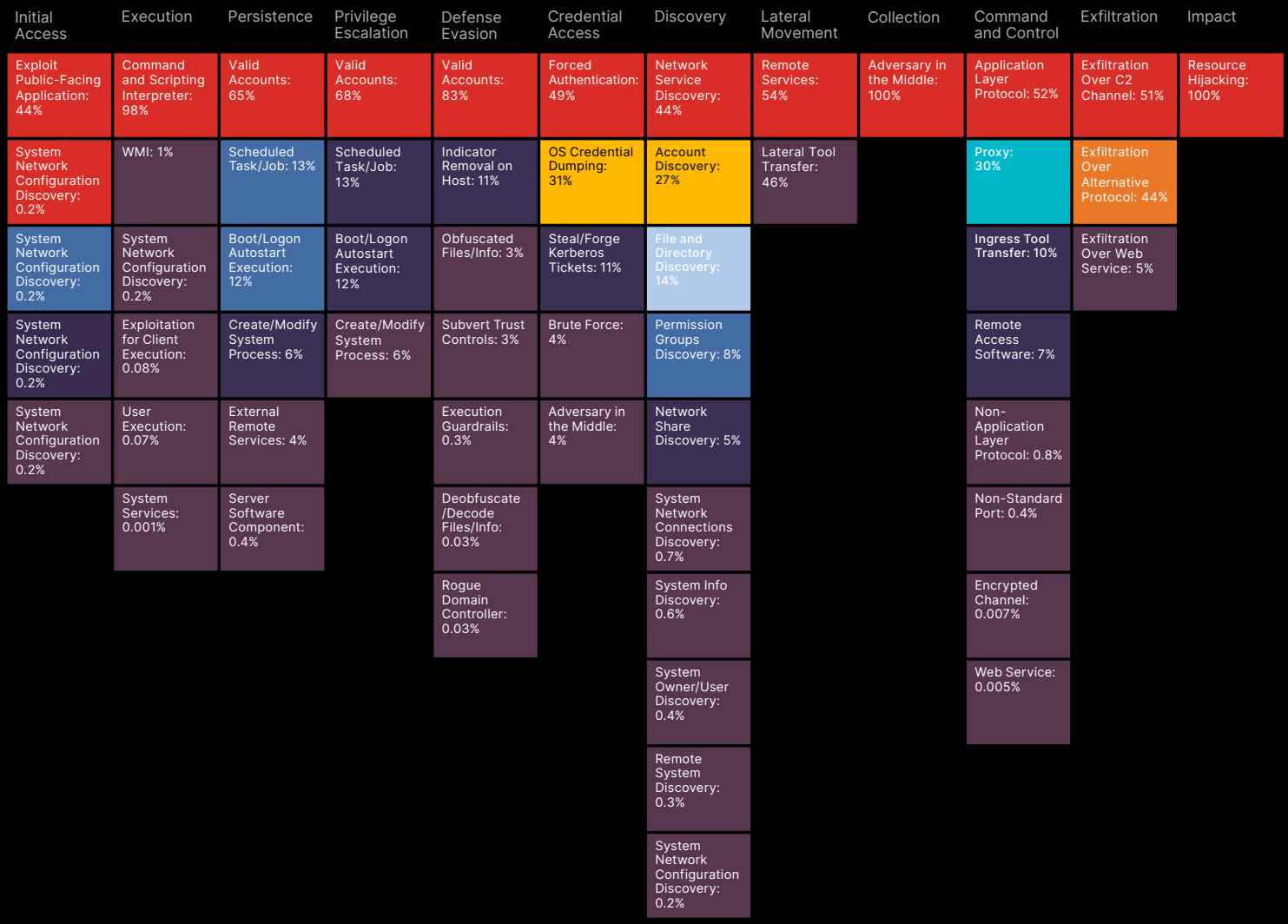
Compartimos esta misma gráfica en nuestro Informe del panorama de amenazas del 1H de 2023 y queríamos destacar los cambios durante el período actual.42 Fabricamos capas de sombra en la parte superior para representar si la clasificación de cada técnica se mantuvo consistente (gris), aumentó (rojo) o disminuyó (azul). Curiosamente, la gráfica revela una consistencia notable en los TTP. Observamos que bastantes de las técnicas que se deslizan por las gráficas se relacionan con la manipulación, manipulación u ofuscación de la información.

Como muestra la gráfica, la mayoría de las tácticas tenían técnicas que mostraban una mayor actividad, y la mayor parte del cambio provino de "Impacto" con "Destrucción de datos" que aumentó drásticamente. Otra técnica que merece atención es "Cuentas válidas", que va del sexto lugar en la lista al tercer lugar. Esto se refiere a adversarios que utilizan credenciales comprometidas, a menudo compradas en la web oscura, para eludir los controles de acceso, crear acceso persistente a sistemas remotos y servicios disponibles externamente, escalar privilegios y evadir la detección.

También vemos algunos cambios entre puestos dentro del "Acceso con credenciales", pero nada que constituya un cambio marítimo. Las técnicas restantes que escalan las gráficas son "Modificar registro" para evadir la detección, lo cual se espera debido al aumento de su prerrequisito típico, "Cuentas válidas" y el uso de "Herramientas de implementación de software" para moverse lateralmente. En algunas campañas de alto perfil, hemos visto a los atacantes usar software de seguridad presente en los entornos de las víctimas para su propio beneficio.

La segunda fuente de observaciones de TTP viene a través de sensores de nube FortiNDR (detección y respuesta de red). Debido a que estas soluciones operan en diferentes capas de la pila, esperaría que su visibilidad de los TTP difiera.

Top ATT&CK techniques observed via FortiNDR



Las diferencias entre los TTP observados por los sandboxes y la tecnología NDR no significan que uno sea mejor o peor que el otro. Cualquier fuente que informe sobre las técnicas "principales" de ATT&CK depende inherentemente del lente a través del cual se ven. El hecho de que "vean" amenazas de manera diferente es un argumento convincente por el que los equipos de seguridad necesitan múltiples capas de detección para obtener una comprensión integral del riesgo de su organización.

Estos son algunos puntos destacados adicionales para considerar específicos para las observaciones de TTP proporcionadas por FortiNDR Cloud:

- Técnicasde C2: Detectamos varias técnicas en la fase C2 del marco MITRE ATT&CK , que incluyen, entre otras, solicitudes DNS Cobalt Strike, túneles DNS y consultas DNS largas. Los atacantes utilizan cada vez más servicios legítimos para C2 y, en algunos casos, ya estamos comenzando a ver la cadena de bloques utilizada para las comunicaciones, ya que esto es resistente al derribo. Glupteba fue el grupo que vimos más recientemente utilizando esta técnica.
- Detecciones de malware: Las RAT como Lokibot y el troyano bancario IcedID continúan teniendo una tendencia en la actividad de detección. Loki es una herramienta de acceso remoto de código abierto con funciones como transferencia de archivos a través de HTTP o SFTP, lanzamiento de un navegador local, toma de capturas de pantalla, ejecución de un registrador de claves y más. Loki a menudo se utiliza como una herramienta posterior a la vulnerabilidad de seguridad para la actividad del equipo rojo o la actividad maliciosa. FortiGuard ATR considera que Loki es de alta gravedad debido a su uso común para el movimiento lateral después de un compromiso de un solo host. El troyano bancario IcedID se conecta a las sesiones del navegador de los usuarios y puede tomar capturas de pantalla para robar credenciales para instituciones financieras. IcedID también se utiliza para facilitar las ofertas de acceso como servicio donde el acceso a redes comprometidas se vende a actores maliciosos adicionales. FortiGuard ATR considera la alta gravedad de IcedID debido al nivel de acceso que otorga a los actores maliciosos tanto al entorno como a la información.
- Evasión de defensa: Tenga en cuenta que la técnica de "Cuentas válidas" que aparece en la fase de "Evasión de defensa" del marco de trabajo MITRE ATT&CK sigue siendo relevante para la posible actividad de amenazas a la que las organizaciones pueden querer prestar atención. Como hemos informado de otras fuentes como FSA y Recon, esta técnica parece ser abusada por actores de amenazas, principalmente impulsada por los Agentes de acceso inicial en la web oscura.

• Ejecución: Detectamos archivos de ejecución portátil (PE) maliciosos conocidos vistos en la red. Un archivo PE es un formato de archivo especializado diseñado para almacenar código ejecutable, código objeto, bibliotecas de enlaces dinámicos (DLL) y recursos similares para su uso en sistemas operativos Windows. Cuando un archivo PE se vuelve malicioso, significa que se ha incrustado código dañino o malicioso dentro de él, lo que potencialmente compromete la seguridad e integridad de cualquier sistema donde se ejecuta el archivo.
• Descubrimiento: FortiNDR Cloud detectó varias enumeraciones sospechosas de Active Directory (AD) y LDAP (listas de usuarios, grupos y confianzas de dominio). Los actores de amenazas pueden usar LDAP y DCE/RPC para enumerar todos los grupos, administradores, usuarios, computadoras, controladores de dominio y confianzas de dominio dentro de un dominio. Después de comprometer una red, los adversarios pueden consultar a AD para obtener una mejor comprensión del diseño y los activos de una organización.

Despegue la luz en la actividad de la Dark Web

Si bien gran parte de nuestra telemetría nos muestra qué acciones han realizado los atacantes en el pasado, la inteligencia de Darknet puede ayudarnos a anticipar lo que los adversarios pueden hacer a continuación. Por primera vez en nuestros informes del panorama de amenazas, compartimos información que hemos recopilado de foros de la web oscura, mercados, canales de telegrama y otras fuentes durante el segundo semestre de 2023 que nos dan una visión de las amenazas emergentes basadas en la charla que ocurre entre los actores de amenazas. Con esta inteligencia, los profesionales de la seguridad pueden protegerse de manera más efectiva contra técnicas y tácticas de ataque nuevas y emergentes.

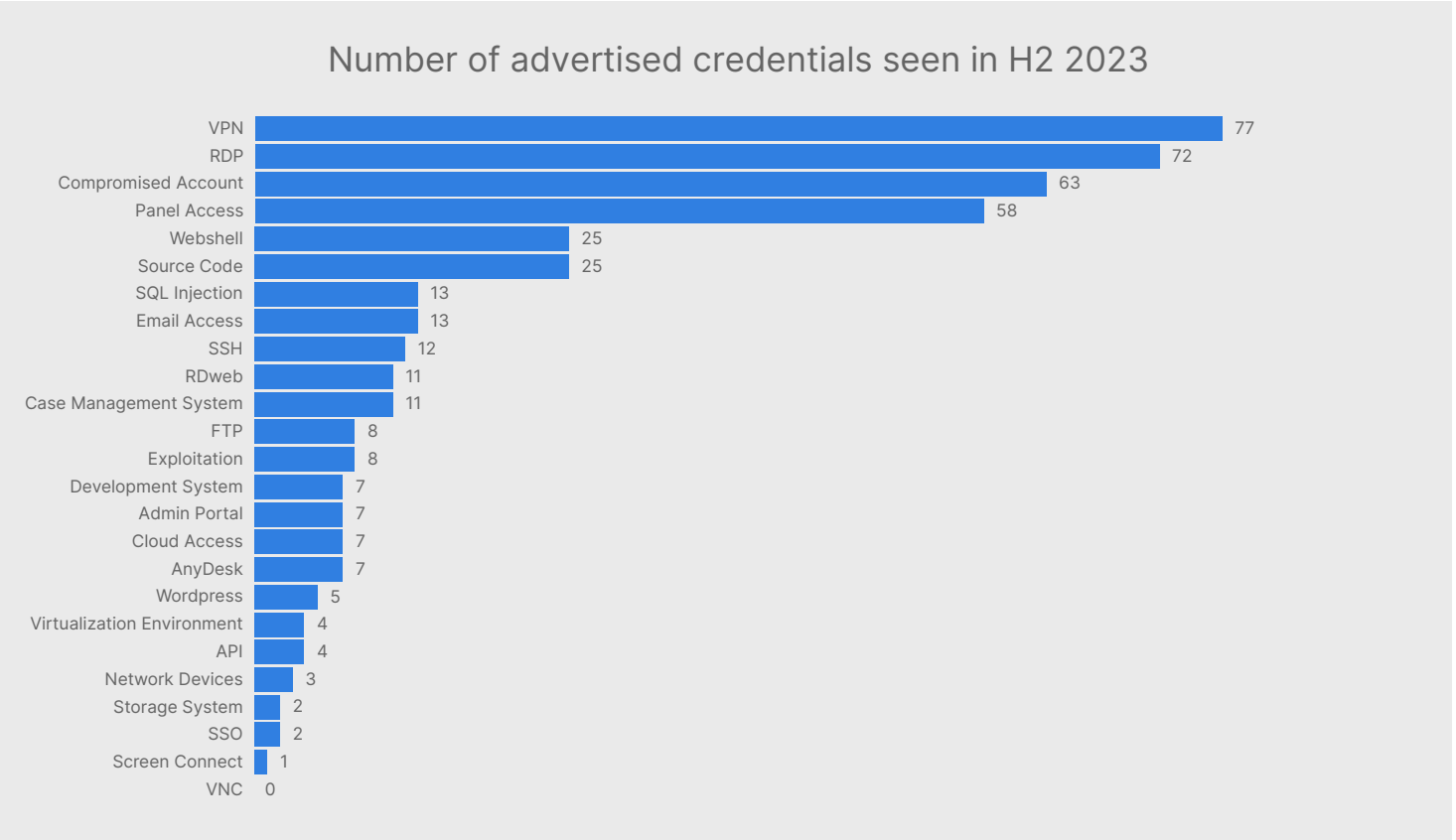
A continuación, presentamos algunos de los hallazgos más frecuentes:

• Los actores de amenazas analizaron con mayor frecuencia cómo dirigirse a organizaciones dentro de la industria de servicios financieros, seguidos de los sectores de servicios empresariales y educación.
• Los actores de amenazas más activos públicamente en toda la web oscura fueron Valerka, Punktir, CoreLab, XXXX y qwer.
• Se compartieron más de 3,000 violaciones de datos en foros destacados de la web oscura.
• De estas violaciones de datos, los actores de amenazas con frecuencia anunciaban el acceso a las organizaciones a través de VPN, RDP y cuentas comprometidas.
• Se analizaron activamente 221 vulnerabilidades en la web oscura, mientras que se analizaron 237 vulnerabilidades en los canales de Telegram.
• Se anunciaron 22 días cero significativos, que afectan a Microsoft Windows, Microsoft Server, Google Chrome, Microsoft Outlook, Adobe Commerce y BIG-IP.
• Se anunciaron para la venta más de 850,000 tarjetas de pago, la mayoría de las cuales eran credenciales de VISA o Mastercard.

Tipos de acceso anunciados en foros de la web oscura

En el segundo semestre de 2023, observamos que los actores de amenazas que operan en la web oscura a menudo anuncian el acceso a las organizaciones a través de VPN, seguido de RDP y cuentas comprometidas:

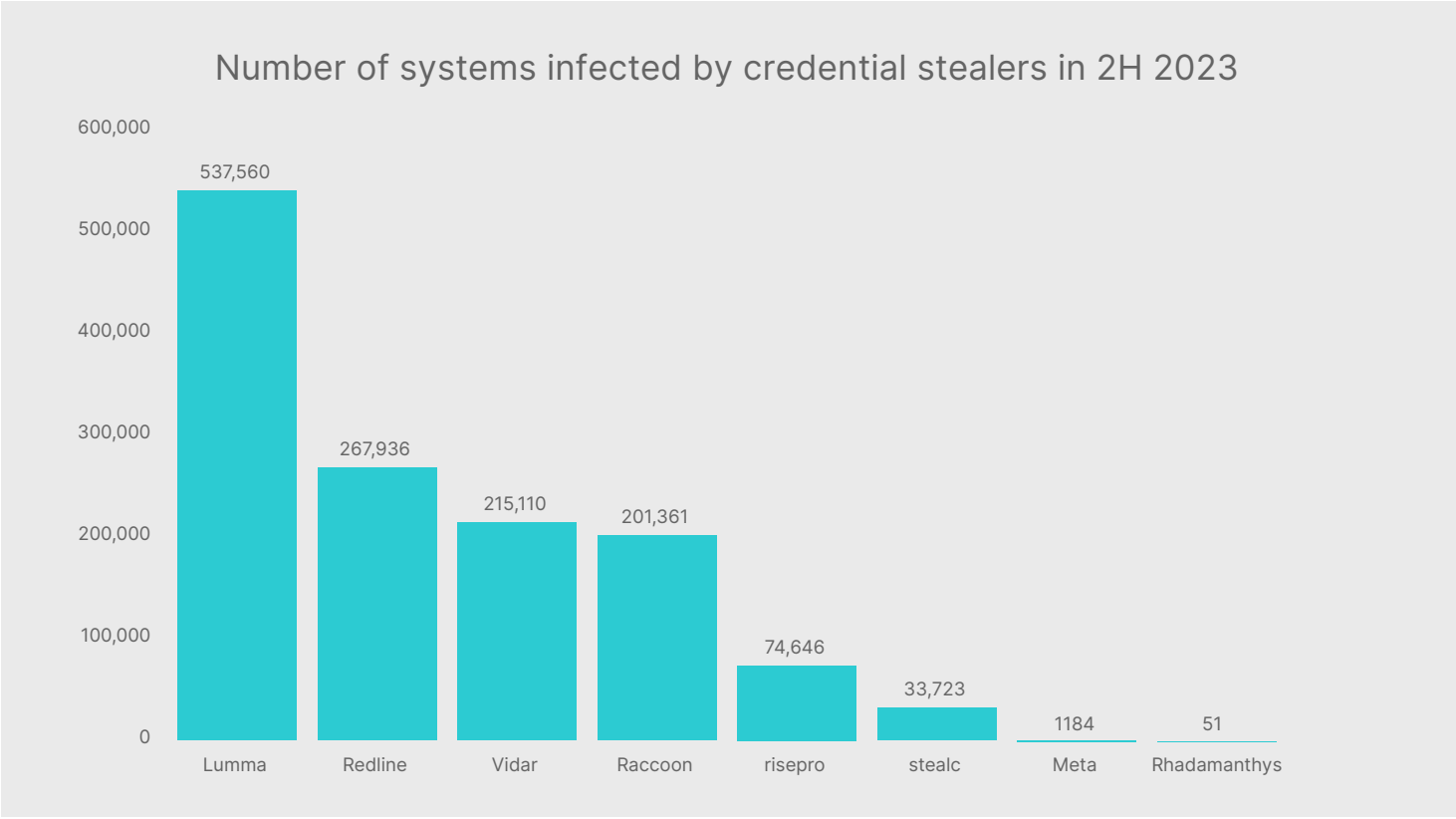
Los precios anunciados para las credenciales de acceso en los foros de Darknet son dinámicos y dependen principalmente de la organización objetivo específica. Varios factores contribuyen a esta estructura de precios, como la valoración de la industria objetivo, su escala, el tamaño de la fuerza laboral y los ingresos anuales. Además, la susceptibilidad de la organización desempeña un papel fundamental en la determinación de los precios que ofrecen los actores de amenazas. El nivel de vulnerabilidad que muestra la organización es otro factor crucial que afecta los precios.



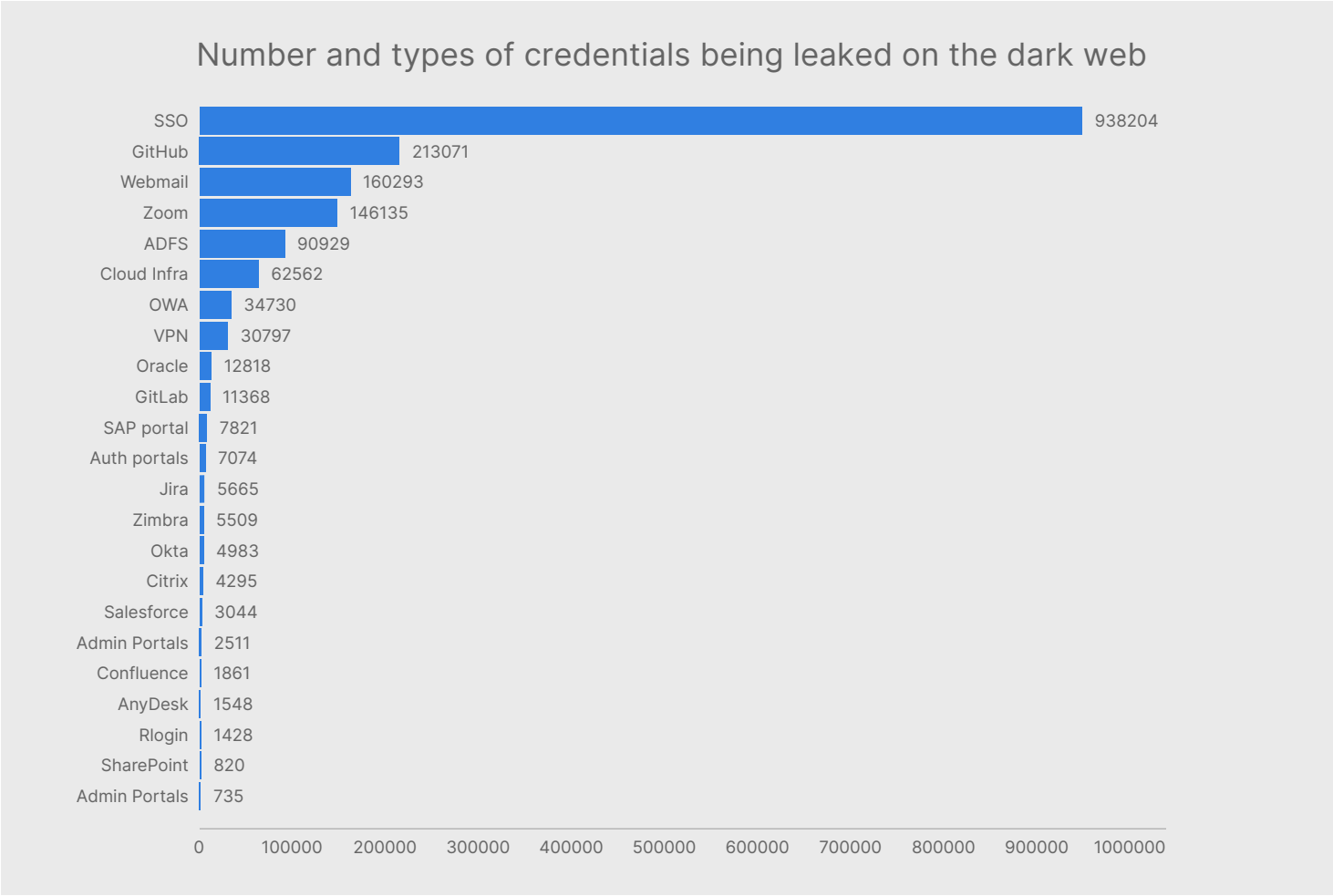
Ladrones de credenciales

Los ladrones de credenciales son un tipo de malware diseñado para robar las credenciales de la cuenta de usuario que, si se adquiere, puede ayudar a un atacante a obtener acceso a sistemas y redes seguros para recopilar información confidencial o crítica. Los datos del sistema del usuario final infectado también se enumeran con frecuencia para la venta en mercados de Darknet de ladrones de credenciales.

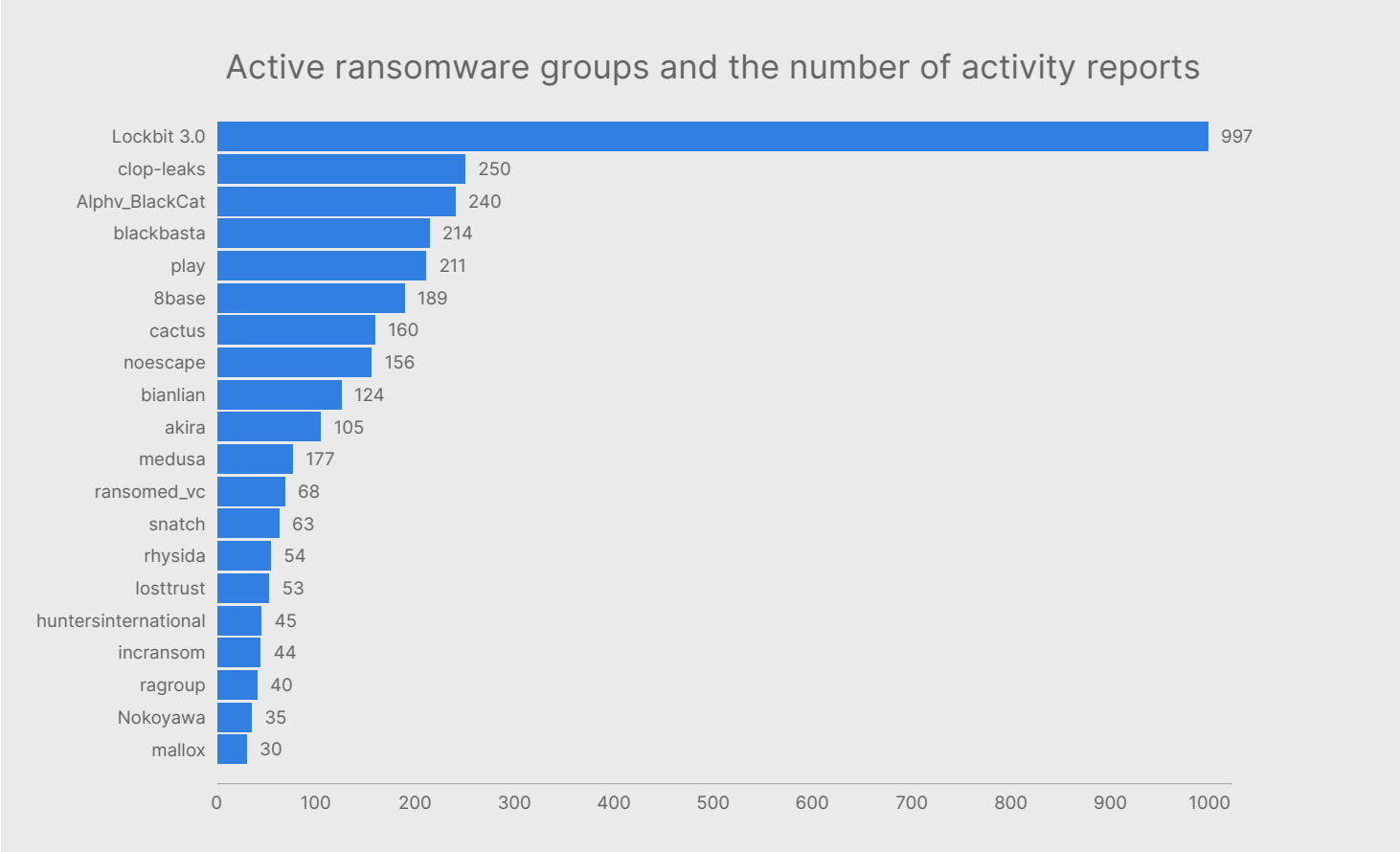
En el 2H de 2023, observamos más de 1,331,571 sistemas infectados por ladrones de credenciales, incluidos Lumma, Redline, Vidar, Racoon, Risepro, stealc, Meta y Rhadamanthys. Estos registros de ladrones están disponibles a precios bajos, lo que permite que un gran número de actores de amenazas los adquieran fácilmente.



También analizamos los tipos y números de credenciales que se filtran en la web oscura:



La siguiente gráfica representa los grupos de ransomware que han estado activos en el 2H de 2023, junto con el recuento respectivo de víctimas:



Tendencias de las zanjas

El equipo de Detección y respuesta administrada (MDR) de FortiGuard administra las instancias de detección y respuesta de endpoint (EDR) en nombre de los clientes de todo el mundo. Sus responsabilidades diarias le dan al equipo una visión significativa de las actividades de los adversarios en los mercados verticales de las empresas y las regiones geopolíticas. De manera similar, nuestro equipo de respuesta a intrusiones (IR) ofrece servicios proactivos y reactivos para apoyar nuestra base global de clientes. La exposición a clientes que luchan activamente contra un incidente de seguridad proporciona una valiosa visión de las intrusiones iniciadas por grupos de APT y actores de amenazas con motivación financiera.

Las siguientes perspectivas proceden de casos del mundo real observados por los equipos de MDR e IR de FortiGuard en el segundo semestre de 2023. Estos hallazgos proporcionan recomendaciones prácticas para responder a características coherentes y emergentes del panorama de amenazas. También nos dan una mejor comprensión de cómo las acciones de los clientes dan forma a las tendencias de amenazas.

Las respuestas con un alcance deficiente generan errores no forzados

Algunas organizaciones no tienen planes o procedimientos de IR adecuados implementados, lo que da lugar a reacciones de golpe de rodilla cuando se produce una violación. Las investigaciones y las acciones de corrección a menudo se dejan incompletas. Las correcciones con un alcance deficiente han dado lugar a que las organizaciones “se arriesguen” inadvertidamente, y los adversarios responden rápidamente al implementar ransomware para causar daños significativos y totalmente innecesarios. Este problema también ocurre cuando las organizaciones aplican tecnologías fuera de su caso de uso previsto, por ejemplo, profesionales que emplean soluciones antivirus heredadas basadas en firmas en un intento por erradicar a un adversario que persiste a través de cargas útiles en la memoria.

Las organizaciones deben asegurarse de tener planes y procedimientos de IR precisos y procesables. Los equipos pueden mejorar significativamente su postura de seguridad empleando de manera eficiente su tecnología existente a través de procedimientos sólidos.

La falta de parches continúa contribuyendo a las intrusiones

En el 86 % de los casos que investigamos, en los que se producía acceso no autorizado a través de la vulnerabilidad, la vulnerabilidad ya se conocía en ese momento y un parche estaba fácilmente disponible. Cuando las organizaciones no responden a la inteligencia frente a amenazas directa y dirigida, es probable que se deba a un problema de recursos. Sin embargo, los líderes deben volver a evaluar sus inversiones en seguridad dado lo vital que es el parcheo regular para protegerse contra las violaciones.

Las copias de seguridad conectadas a la producción son objetivos atractivos para los atacantes

Los miembros de nuestro equipo de IR han trabajado con algunas víctimas de ransomware que han invertido en soluciones de respaldo que se autentican con su entorno corporativo principal y permanecen conectadas las 24 horas del día, los 7 días de la semana. En estos casos, los actores de amenazas involucrados pudieron acceder, manipular y cifrar las soluciones de copia de seguridad durante las intrusiones, haciéndolas inútiles. Los actores de amenazas a menudo buscan activamente copias de seguridad para inhibir la recuperación del sistema. Las organizaciones deben asegurarse de que sus copias de seguridad estén adecuadamente separadas de la red.

Los procesos de eliminación automatizados pueden obstaculizar las investigaciones

En muchas ocasiones, nuestro equipo de IR trabajó con organizaciones que habían configurado sus herramientas antivirus para eliminar automáticamente archivos maliciosos al detectarlos, en lugar de ponerlos en cuarentena. Esta regla de eliminación automática evita la atribución adecuada de la actividad observada, lo que puede ralentizar una investigación. Esto también puede afectar a los equipos de seguridad que pueden no poder realizar correctamente el triaje una vez que estos artefactos se hayan eliminado. Recomendamos que las organizaciones pasen a una configuración que pone en cuarentena las muestras y almacena una copia (o al menos recopila hashes de archivos) para que los equipos de IR puedan usar métodos de recuperación alternativos si es necesario.

Los servidores ESXi son vacas de efectivo para operadores de ransomware

Los servidores ESXi están siendo cada vez más atacados durante los ataques de ransomware. (ESXi es un hipervisor de metal desnudo que puede particionar un servidor en múltiples máquinas virtuales). Los servidores ESXi ofrecen a los adversarios una gran ventaja por su dinero dado el impacto significativo que pueden tener en la capacidad de una organización para realizar negocios cuando se ven comprometidos. El lanzamiento de creadores como el ransomware Babuk y HelloKitty, que se puede utilizar para dirigirse a servidores ESXi, ha hecho que sea más fácil que nunca que los adversarios con motivos financieros se dirijan a estos dispositivos.

Las cuentas válidas continúan proporcionando vías rápidas a través de las cadenas de eliminación

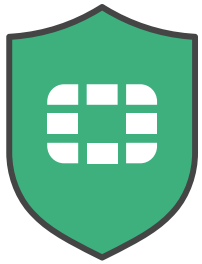
Los atacantes continúan haciendo mal uso de cuentas válidas para moverse lateralmente a través de entornos comprometidos. Los actores de amenazas utilizan estas cuentas válidas en combinación con las técnicas de LoLbins para evadir las defensas de las organizaciones. Como resultado, las organizaciones deben monitorear el uso sospechoso de cuentas válidas dentro de su entorno.

Los adversarios utilizan cada vez más los servicios de Microsoft Windows para ejecutar RAT

Hubo un ligero aumento en la prevalencia de los servicios de Microsoft Windows que se utilizan como método de ejecución principal para RAT dentro del entorno de una víctima. La ejecución del servicio se puede utilizar para la escalada de privilegios y puede abstraer la ejecución en las cadenas de proceso RAT, ocultando las actividades maliciosas y aumentando las complejidades para los equipos de seguridad que tienen la tarea de clasificar un incidente. Esto a menudo da lugar a una investigación incompleta por parte de equipos que carecen de los recursos para respaldar el análisis en profundidad requerido para vincular la actividad anómala del servicio a cuentas comprometidas y puntos de ingreso. La ejecución del servicio es fácil de implementar y, dada la naturaleza de servicio pesado de las versiones más recientes de Microsoft Windows, los adversarios probablemente la ven como otra oportunidad para evadir la detección.

Los actores de amenazas utilizan regularmente herramientas de administración de código abierto

Los actores de amenazas y los grupos de APT continúan utilizando herramientas de administración de código abierto conocidas para comprometer a las víctimas desprevenidas. El uso de estas herramientas es constantemente alto para muchas etapas de una intrusión, desde el descubrimiento hasta el movimiento lateral. Las herramientas de código abierto suelen ser ligeras y a menudo pueden pasar desapercibidas en organizaciones que no comprenden la amenaza que representan. El problema de identificar el uso sospechoso de estas herramientas se vuelve más complejo por el uso legítimo de software de código abierto por parte de los administradores del sistema. Las organizaciones deben tratar de caracterizar el uso legítimo de estas herramientas y utilizar técnicas de control de aplicaciones para bloquear el uso anómalo.



Para recibir notificaciones cuando detectemos una amenaza nueva o emergente, regístrese aquí para recibir alertas de brotes de FortiGuard Labs. También puede descargar el Informe anual de alertas de brotes de 2023 aquí.

Conclusión

Esperamos que esta edición del informe del panorama de amenazas de Fortinet proporcione información valiosa para ayudarlo a priorizar e implementar medidas de seguridad adecuadas dentro de su organización. En resumen, estas son las tres tendencias principales que observamos durante el segundo semestre de 2023 que nos destacaron más. Tenga esto en cuenta y ajuste su estrategia de gestión de riesgos en consecuencia.

La zona roja permanece estable. El panorama de amenazas generalmente se define por un cambio constante, por lo que es inusual encontrar algo estático. La proporción de vulnerabilidades observadas con vulnerabilidades de seguridad conocidas se ha desplazado alrededor del 8 % desde que comenzamos a medirlas inicialmente hace casi dos años. Las vulnerabilidades en sí cambian, por supuesto, pero el esfuerzo general requerido para corregirlas aparentemente no lo hace. Aproveche esta previsibilidad para asignar recursos para minimizar la zona roja de su organización.

Mantenga las “viejas” vulnerabilidades en su radar. Las nuevas vulnerabilidades de seguridad y malware pueden propagarse lejos y rápidamente, por lo que si su organización tiende a estar entre los primeros objetivos, puede ser solo una cuestión de horas o días antes de que los ataques lleguen a su camino. Sin embargo, también hemos visto que muchas vulnerabilidades, incluso las que existen desde hace años, a menudo permanecen en el radar de los actores de amenazas como objetivos activos. Desafortunadamente, esto significa que no puede estar tan enfocado en protegerse contra nuevas vulnerabilidades y ataques que descuida los antiguos. Los equipos de seguridad exitosos deben protegerse contra todo el ciclo de vida de las vulnerabilidades de seguridad, y esto comienza con un programa proactivo de parches y actualizaciones.

Las industrias críticas son los principales objetivos de ransomware. Los actores detrás de las campañas de ransomware siempre han sido industriosos. Ya sea haciendo ajustes rápidos a las demandas de rescate basados en la dinámica del mercado de criptomonedas o creando grandes empresas criminales para minimizar el costo y maximizar la escala, tienen una tendencia a hacer que las cosas sucedan. Eso es lo que hace que el cambio continuo a dirigirse a industrias críticas sea aún más preocupante. Estos entornos con mucho volumen de TO son particularmente susceptibles a costosas interrupciones, lo que aumenta en gran medida la presión de pagar altos rescates para restaurar la productividad.

Si bien cada uno de nosotros tiene una función vital que desempeñar en la lucha contra nuestros adversarios colectivos, ninguna organización puede detener a los actores de amenazas de manera autónoma. La inteligencia compartida es una parte crucial de cómo garantizamos respuestas oportunas y precisas cuando los atacantes atacan. Cuanto más colaboremos en los sectores público y privado, más efectivos podremos ser para interrumpir el cibercrimen.

Notas al pie

1 Alertas de brotes de FortiGuard, FortiGuard Labs, consultado el 18 de febrero de 2024.

2 Zyxel Multiple Firewall Vulnerabilities, FortiGuard Outbreak Alerts, 6 de junio de 2023.

3 Zyxel Router Command Injection Attack, FortiGuard Outbreak Alerts, 9 de agosto de 2023.

4 Zerobot Attack, FortiGuard Outbreak Alerts, 27 de diciembre de 2022.

5 Vulnerabilidad de inyección de comandos de operaciones para redes VMware Aria, Alertas de brotes de FortiGuard, 22 de junio de 2023.

6 Vulnerabilidad de ejecución de código IBM Aspera Faspex, Alertas de brotes de FortiGuard, 1 de marzo de 2023.

7 Cisco IOS XE Web UI Attack, FortiGuard Outbreak Alerts, 20 de octubre de 2023.

8 Citrix Bleed Attack, FortiGuard Outbreak Alerts, 2 de noviembre de 2023.

9 Apache RocketMQ Remote Command Execution Vulnerability, FortiGuard Outbreak Alerts, 5 de julio de 2023.

10 Progress MOVEit Transfer SQL Injection Vulnerability, FortiGuard Outbreak Alerts, 5 de junio de 2023.

11 MITRE ATT&CK, consultado el 18 de febrero de 2024.

12 JS/Agent.CY!tr, FortiGuard Labs Encyclopedia, 9 de junio de 2022.

13 JS/Agent.F022!tr, FortiGuard Labs Encyclopedia, 10 de julio de 2023.

14 JS/Agent.PIV!tr, FortiGuard Labs Encyclopedia, 1 de noviembre de 2021.

15 JS/Agent.NDS!tr, FortiGuard Labs Encyclopedia, 7 de noviembre de 2023.

16 JS/ScrInject.B!tr, FortiGuard Labs Encyclopedia, 30 de agosto de 2011.

17 Ibid.

18 JS/Cryxos.5478!tr, FortiGuard Labs Encyclopedia, 30 de marzo de 2021.

19 CVE-2023-46604, NIST National Vulnerability Database, consultado el 18 de febrero de 2024.

20 Lucian Constantin, HelloKitty Ransomware Deployed Via Critical Apache Active MQ Flaw, CSO Online, 2 de noviembre de 2023.

21 Apache ActiveMQ Ransomware Attack, FortiGuard Outbreak Alerts, 6 de noviembre de 2023.

22 Lazarus RAT Attack, FortiGuard Outbreak Alerts, 12 de diciembre de 2023.

23 Ataque de malware del agente, alertas de brotes de FortiGuard, 7 de septiembre de 2023.

24 CVE-2017-11882, NIST National Vulnerability Database, consultado el 18 de febrero de 2024.

25 CVE-2018-0802, NIST National Vulnerability Database, consultado el 18 de febrero de 2024.

26 CVE-2017-9841, NIST National Vulnerability Database, consultado el 18 de febrero de 2024.

27 CVE-2018-15133, NIST National Vulnerability Database, consultado el 18 de febrero de 2024.

28 CVE-2021-41773, NIST National Vulnerability Database, consultado el 18 de febrero de 2024.

29 Cedric Pernet, Androxgh0st Malware Botnet Steals AWS, Microsoft Credentials and More, TechRepublic, 18 de enero de 2024.

30 Ravie Lakshmanan, New Version of Prometei Botnet Infects Over 10,000 Systems Worldwide, The Hacker News, 10 de marzo de 2023.

31 El economista subterráneo: Volumen 3, Edición 12, ZeroFox, 27 de junio de 2023.

32 Kevin Poireault, DarkGate and PikaBot Activity Surge in the Wake of QakBot Takedown, Infosecurity Magazine, 21 de noviembre de 2023.

33 Índice de vulnerabilidades y exposiciones comunes, MITRE , consultado el 18 de febrero de 2024.

34 Douglas José Pereira dos Santos, 2H de 2022 Informe del panorama global de amenazas: Información clave para CISO, Fortinet, 3 de marzo de 2023.

35 CVE-2021-44228, NIST National Vulnerability Database, consultado el 18 de febrero de 2024.

36 CVE-2023-44487, NIST National Vulnerability Database, consultado el 18 de febrero de 2024.

37 Sistema de puntuación de predicción de vulnerabilidades de seguridad, Forum of Incident Response and Security Teams, consultado el 18 de febrero de 2024.

38 CVE-2023-28121, NIST National Vulnerability Database, consultado el 18 de febrero de 2024.

39 El Informe global de ransomware 2023, Fortinet, 20 de abril de 2023.

40 Ransomware Extortion Skyrockets in 2023, Reaching $449.1M and Counting, The Hacker News, 12 de julio de 2023.

41 MITRE ATT&CK, consultado el 18 de febrero de 2024.

42 FortiGuard Labs 1H 2023 Threat Landscape Report, Fortinet, 7 de agosto de 2023.

www.fortinet.com