SOPHOS
Cybersecurity delivered.

Informe de Sophos sobre amenazas 2023

Los mercados delictivos maduros presentan nuevos retos para los responsables de la seguridad

Sophos X-Ops

Contenido

Carta del director tecnológico 2

Marcando la tónica: la guerra en Ucrania 4
- Un conflicto regional con repercusión mundial 4
- En el centro de las cosas 5

La economía del malware 6
- Los nueve malvados 6
- Evolución hacia una profesionalización sofisticada 11
- Ladrones de información 13

Evolución del ransomware 17

Herramientas de ataque 20

El uso malintencionado de las herramientas de seguridad ofensiva 21
- Otras herramientas de seguridad usadas de forma malintencionada 24
- RAT de doble uso 24
- Binarios LOLBin y ejecutables legítimos 25
- Vulnerabilidades «propias» 26
- Ransomware dirigido contras las actualizaciones de seguridad de endpoints 28
- Malware minero 28

Más allá de Windows: panorama de amenazas para Linux, Mac y dispositivos móviles 30
- Amenazas para Linux 30
- Amenazas para dispositivos móviles 33

Conclusión 34

Joe Levy
Sophos CTO

Carta del director tecnológico

La industria de la ciberseguridad tiende en la recta final del año, todos los años, a echar la vista atrás y proclamar que los últimos doce meses han sido de los más trascendentales en la historia de la industria. Aunque 2022 no ha tenido sucesos señalados como Aurora, Stuxnet, WannaCry o el ciberataque a Colonial Pipeline, lamentablemente se ha ganado su lugar en los anales de la ciberhistoria al estallar una guerra en Europa, la mayor en medio siglo.

El motivo por el que esto es importante para la ciberseguridad es que un país bien conocido como uno de los principales promotores y refugios de la actividad cibercriminal del mundo, el primogenitor del ransomware como industria nacional de facto, invadió a su vecino.

Una vez que Rusia invadió Ucrania, era inevitable que el gobierno ruso alentara (o reclutara directamente) a organizaciones de ciberdelincuencia nacionales para inclinar la opinión mundial a su favor, al tiempo que intentaba sabotear las simpatías que el presidente de Ucrania pudiera haber cosechado a nivel mundial. Que es exactamente lo que sucedió cuando grupos de ransomware, malware y desinformación se unieron para apoyar la agresión rusa.

Este esfuerzo, hasta el momento, ha resultado ser un fracaso total. La opinión mundial sobre los delincuentes de ransomware ya estaba por los suelos cuando, durante la pandemia, distintos grupos atacaron las partes más vulnerables de los sectores empresariales más cruciales implicados en la respuesta a la misma, incluyendo la industria de la salud, las organizaciones de investigación médica, las empresas críticas para mantener las cadenas de suministro y las actividades relacionadas con la alimentación y la energía, e incluso los sistemas educativos. Las bandas de ransomware no habían atraído precisamente la simpatía de la opinión pública, cuando enojaron aún más al mundo al pronunciar su apoyo inquebrantable a la invasión rusa y declarar como objetivo a cualquier país u organización que se les opusiera.

Pero otros miembros de estos mismos grupos, basados en Ucrania, veían las cosas de forma algo distinta. Y se inició un tira y afloja de filtraciones, que reveló la información más delicada jamás divulgada hasta ese momento sobre la forma de operar de los grupos de ciberdelincuentes de ransomware. Parece que con la guerra se han roto los lazos entre los ciberdelincuentes ucranianos y sus homólogos rusos (y bielorrusos), posiblemente para siempre.

De forma paralela, durante todo este tiempo en que Rusia ha estado preocupada promoviendo su guerra de agresión, China ha estado realizando maniobras ciberdelictivas de gran calado, dirigidas no solo a sus vecinos y a los países que considera cruciales en su «Iniciativa de la Franja y la Ruta», sino a la propia industria de la seguridad. En una serie de ataques cada vez más descarados contra las empresas que están en primera línea de la protección de la información y las redes, grupos de ciberdelincuentes radicados en China (y probablemente patrocinados por esta) han estado atacando los productos de seguridad de hardware fabricados por casi todas las empresas de los sectores de la ciberseguridad y las infraestructuras.

En un sentido muy real y muy personal, da la impresión de que en este 2022 se han acabado las contemplaciones, y las dos mayores naciones que suponen una amenaza para la ciberseguridad del resto del mundo han decidido dejar de fingir que no están implicadas en las filtraciones importantes, los grandes ataques a las infraestructuras o las perturbaciones en la educación, el comercio mundial o la asistencia sanitaria. Incluso podrían estar jactándose de ello en nuestras caras, como diciendo ¿qué vais a hacer al respecto?

Lo que hemos estado haciendo al respecto, y lo que Sophos va a seguir haciendo, es reforzar nuestras iniciativas ya en marcha para proteger tanto a nuestros clientes como a nosotros mismos. La empresa ha emprendido un proceso de varios años de duración de mejora incremental de la detección y la intervención automatizada del comportamiento del ransomware, llegando a tener tanto éxito en sabotear a los atacantes que ahora esos adversarios activos centran sus esfuerzos cada vez más en evadirnos antes de poder materializar cualquier amenaza.

A la vez, a la vista de los ataques contra las infraestructuras de seguridad por parte de grupos de delincuentes basados en China y Rusia, la confianza en nuestros proveedores es más importante que nunca. Creemos que los proveedores deben comunicar sus inversiones en seguridad con transparencia para ganarse esa confianza y mantenerla, especialmente cuando el proveedor se dedica a proveer servicios y productos de ciberseguridad. Sophos mantiene un Trust Center que profundiza en nuestro trabajo en materia de avisos y divulgación de información, nuestras pruebas de seguridad y el programa de recompensas por la detección de errores, y nuestros planes de análisis y respuesta a incidentes. Invertimos continuamente en la protección de nuestra propia infraestructura contra ataques selectivos de APT, y en reforzar el hardware y el software ejecutado en los entornos de nuestros clientes. El éxito en este aspecto será gradual, ya que los adversarios no han dejado de intentar descubrir y explotar vulnerabilidades y, de hecho, parece que han intensificado sus esfuerzos diseñados para socavar la seguridad de los firewalls, switches y puntos de acceso a las redes de todos y cada uno de los proveedores. También continuamos impulsando las configuraciones seguras por defecto en nuestras ofertas, e introducimos comodidades como la comprobación del estado de seguridad y las correcciones de políticas en nuestros productos y servicios para mejorar la postura operativa y la higiene.

Las amenazas seguirán evolucionando, y Sophos se adaptará sin descanso para seguir proporcionando resultados superiores en ciberseguridad.

Marcando la tónica: la guerra en Ucrania

Si la guerra es la continuación de la política pero con otros medios, y el ciberconflicto es solo otro aspecto del enfrentamiento armado, tiene sentido que el conflicto de Ucrania tenga el mismo cariz tanto en la red como en la realidad. En el momento de escribir este informe, el panorama de amenazas dentro de las fronteras de Ucrania no es nada halagüeño, y en el resto de occidente, a pesar de suponer trastornos menos generalizados aunque significativos, constituye un motivo de preocupación, ya que el potencial de ampliación del conflicto, la desinformación y las perturbaciones siguen siendo altos.

Un conflicto regional con repercusión mundial

Tal como era de esperar, la escalada cinética del ataque ruso a Ucrania el 24 de febrero sacó a escena a los estafadores para aprovecharse del dolor y la preocupación globales.

A principios de marzo, detectamos un repunte de falsos correos benéficos solicitando donaciones internacionales para Ucrania. En aquellos primeros días de la guerra, las autoridades ucranianas hicieron llamamientos al mundo solicitando donaciones para ayudar a sus esfuerzos de defensa, y esos llamamientos incluían peticiones para donar criptodivisas al tesoro del país. Los estafadores aprovecharon inmediatamente el cebo de las criptomonedas y enviaron millones de mensajes de spam repitiendo la petición, pero intercambiando las direcciones de los monederos de criptomonedas por otras que no estaban asociadas con el gobierno ni con ninguna otra organización benéfica legítima o agencia de ayuda no gubernamental. El fin de semana del 5 y 6 de marzo, el volumen de spam que solicitaba donaciones para estos falsos monederos de criptomonedas fue tan grande que constituyó la mitad de todo el spam que recibimos en ese periodo de tiempo, una cantidad sorprendentemente grande. Afortunadamente, la intensidad de la campaña se redujo a los pocos días.

Estafas relacionadas con Ucrania como porcentaje del volumen diario de spam, marzo de 2022

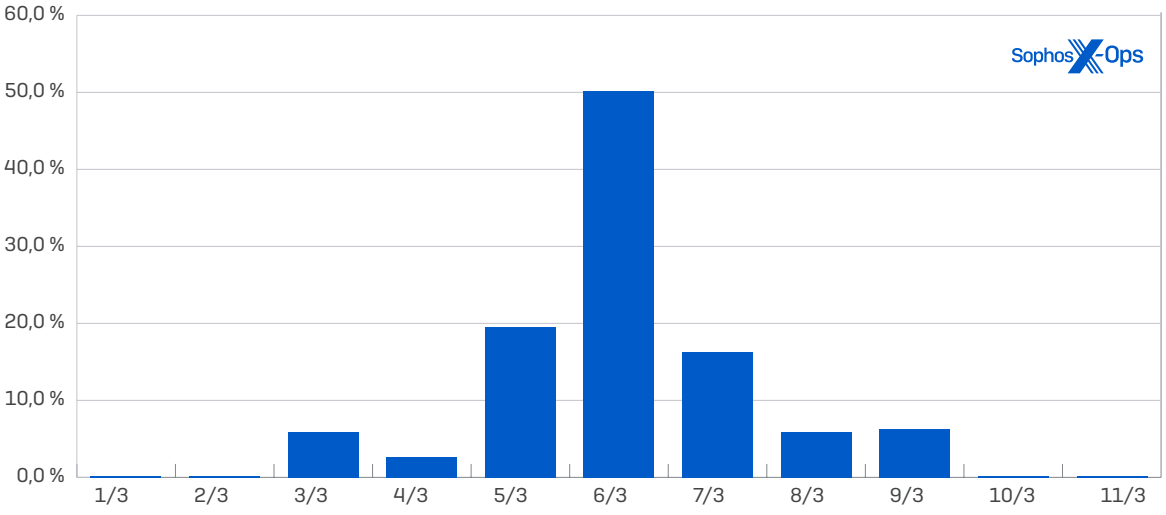

Fig. 1. El volumen de correos electrónicos de spam solicitando donaciones a direcciones de criptomonedas falsas experimentó un repunte acusado, aunque corto.

En mayo también habían aparecido cientos de páginas falsas solicitando «donaciones», pero como ocurrió con el spam inicial, a juzgar por los puntos en común de los datos de pago, probablemente estaban gestionadas por relativamente pocos grupos. El factor impulsor en estos ataques no implicaba ninguna sofisticación técnica importante. En su lugar, los ataques usaban el nombre del país o de sus líderes como cebo y se basaban en vulnerabilidades y exploits relativamente antiguos para lograr su objetivo.

Por ejemplo, en una destacada campaña de spam ese mes, el grupo de malware Emotet distribuyó una colección de documentos Word maliciosos con títulos provocativos que imitaban la propaganda rusa, por ejemplo, «Los EE. UU. y los aliados proporcionan armas químicas a los militares ucranianos.doc», en un intento de propagar su malware. Los documentos maliciosos en ese ataque aprovechaban un exploit CVE-2021-40444 para infectar los ordenadores de las víctimas que abrían los documentos en equipos que no tenían instalado el parche de Office, publicado el otoño anterior.

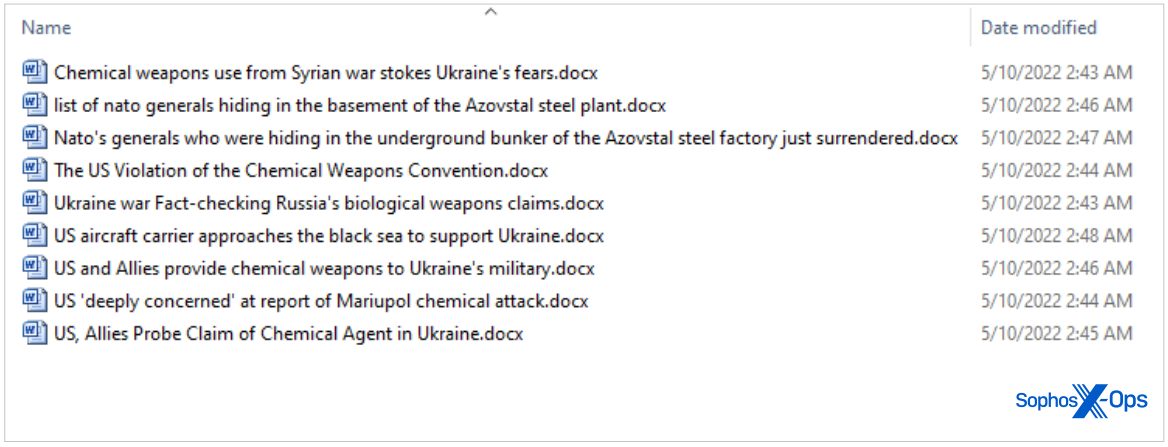

Fig. 2. Títulos de los documentos en el spam malicioso de Emotet con la temática de Ucrania con afirmaciones falsas y aterradoras.

En lo que se refiere a los ciberataques a nivel estatal fuera de las fronteras de Ucrania, en el momento de redactar este informe la atribución de uno de los dos incidentes de mayor repercusión no es nada sólida. El ataque a ViaSat, que afectó a los servicios por satélite para los ucranianos y también para clientes en otras partes de Europa horas antes del inicio de la invasión, es considerado categóricamente por las autoridades como obra de los rusos. Pero los ataques de tipo *defacement* a los sitios web públicos de aeropuertos occidentales sucedidos en octubre son más difíciles de interpretar: ¿fue un ataque a nivel gubernamental para intimidar a los aliados de Ucrania o fueron ataques independientes?

Es razonable, de hecho, actuar como si se tratase de esto último. Los ataques DDoS y de tipo *defacement* tecnológicamente sencillos (que también afectaron a sitios web de aeropuertos, por no mencionar el intento de alterar la votación de Eurovisión) fueron otro aspecto de los primeros días de la guerra, pero a medida que el conflicto se encamina hacia otro invierno y las tensiones globales son altas, algunos observadores no especializados consideran que las bufonadas del grupo con afiliación rusa KillNet interrumpiendo páginas web son un recordatorio de que en ese frente todavía no se ha resuelto nada.

En el centro de las cosas

Dentro de Ucrania, el panorama es mucho más oscuro y extraño. Varios ataques dirigidos contra el gobierno ucraniano han seguido los patrones vistos en campañas delictivas: el uso de correos electrónicos de ingeniería social, malware genérico y herramientas comerciales de seguridad ofensiva explotadas. En un caso, un correo electrónico falsificado contenía un enlace a una «actualización de antivirus» que en realidad distribuía una carga para Cobalt Strike. En otro (que examinaremos más adelante en este informe), un ladrón de información afirmaba tener a la venta cantidades importantes de datos sobre organizaciones gubernamentales y ciudadanos ucranianos: sin ninguna demanda de rescate concreta, solo una filtración para exponer los datos.

Mientras tanto, Ucrania y Rusia, a pesar de ser países independientes, tienen ciudadanos que han sido cómplices criminales (literalmente) durante mucho tiempo, con múltiples bandas de ransomware usando afiliados procedentes de ambas naciones. Cuando estalló la guerra, parece ser que algunas bandas se desintegraron debido a estallidos de nacionalismo.

Más espectacular todavía, las divisiones entre los miembros rusos y ucranianos de las bandas de ransomware y sus afiliados pueden haber conducido a la formación de Conti Leaks, un volcado de registros de chats del grupo de ransomware. Posteriormente, una cuenta de Twitter efímera denominada @TrickbotLeaks doxeó (reveló información personal o privada sobre) presuntos miembros de los grupos delictivos Trickbot, Conti, Mazo, Diavol, Ryuk y Wizard Spiders.

¿Qué podemos deducir de este drama? Una prueba más de que, como muchos investigadores occidentales llevan diciendo desde hace años, el Servicio Federal de Seguridad de Rusia (FSB) está estrechamente vinculado a un número de grupos de ransomware, y que incluso podría haber contratado a algunas de esas entidades para incursiones específicas con Conti.

Desafortunadamente, ninguno de estos conflictos internos ha conllevado una reducción importante ni duradera de la actividad de ransomware a nivel global. Y aunque 2022 comenzó con múltiples detenciones por parte de oficiales del FSB de miembros del grupo de ransomware como servicio REvil (en enero) y una banda de carding (fraude basado en tarjetas de crédito) anónima (en febrero), e incluso con la extradición de un miembro de REvil a los EE. UU. para su juicio a principios de marzo, a mediados de año ese tipo de colaboración internacional en la lucha contra el crimen ya parecía algo impensable, y había indicios de que REvil, o algo que pretendía ser ese servicio, ya había renacido de nuevo. Y la guerra continúa.

La economía del malware

Aunque este último año han evolucionado numerosos aspectos del panorama de las amenazas, el más significativo probablemente sea el desarrollo continuado de la economía de la ciberdelincuencia. Este ecosistema se ha ido transformando cada vez más en una industria en sí misma, con una red de servicios de soporte y enfoques operativos profesionalizados y sólidos.

De la misma forma que las empresas de tecnologías de la información han evolucionado hacia ofertas «como servicio», también lo ha hecho el ecosistema de la ciberdelincuencia. Los brókeres de acceso, el ransomware, el malware para robar información, la distribución de malware y otros elementos de las operaciones de la ciberdelincuencia han facilitado la entrada a los atacantes en potencia.

Esta tendencia la está impulsando en parte la emergente economía de la ciberdelincuencia. Mercados ilícitos como Genesis permiten a los ciberdelincuentes principiantes comprar malware y servicios de despliegue de malware y, a su vez, vender credenciales y otros datos robados de forma masiva. Los brókeres de acceso utilizan exploits genéricos de software vulnerable para establecerse en cientos de redes y vender a continuación ese acceso a otros delincuentes, frecuentemente vendiendo el mismo acceso explotado múltiples veces. Y afiliados del ransomware y otros atacantes compran credenciales y accesos para realizar actividades delictivas de más riesgo y con una recompensa superior.

La industrialización del ransomware ha permitido que «afiliados» del ransomware evolucionen hasta convertirse en entidades profesionales especializadas en el uso de exploits. Utilizando herramientas de seguridad ofensiva profesionales, software legítimo de administración y de soporte técnico, malware como servicio y otros exploits y malware obtenidos en el mercado, hemos visto cómo los delincuentes convergen alrededor de conjuntos de herramientas, tácticas y prácticas que ya no se pueden asociar a determinadas operaciones específicas de ransomware, espionaje vinculado a un estado ni otros motivos concretos. Estos grupos profesionalizados se especializan en obtener (o comprar) el acceso para cualquier delincuente motivado dispuesto a pagar o, en algunos casos, múltiples delincuentes con múltiples motivos.

Estos grupos han imitado en muchas aspectos a la industria de la nube y los servicios web en sus modelos de negocio. Del mismo modo que en el ámbito de TI de las organizaciones se ha adoptado el modelo «como servicio» para un número de operaciones creciente, prácticamente cualquier aspecto del kit de herramientas para la ciberdelincuencia se puede externalizar a proveedores de delincuencia como servicio que se publicitan en sitios web clandestinos. Trataremos brevemente nueve variaciones de estos servicios y desarrollaremos una décima de forma más detenida.

Los nueve malvados

Acceso como servicio: el acceso a cuentas y sistemas comprometidos se vende de forma individual o masiva a través de servicios clandestinos, incluyendo credenciales del protocolo de escritorio remoto (RDP) y VPN, cuentas, bases de datos, shells web y vulnerabilidades explotables.

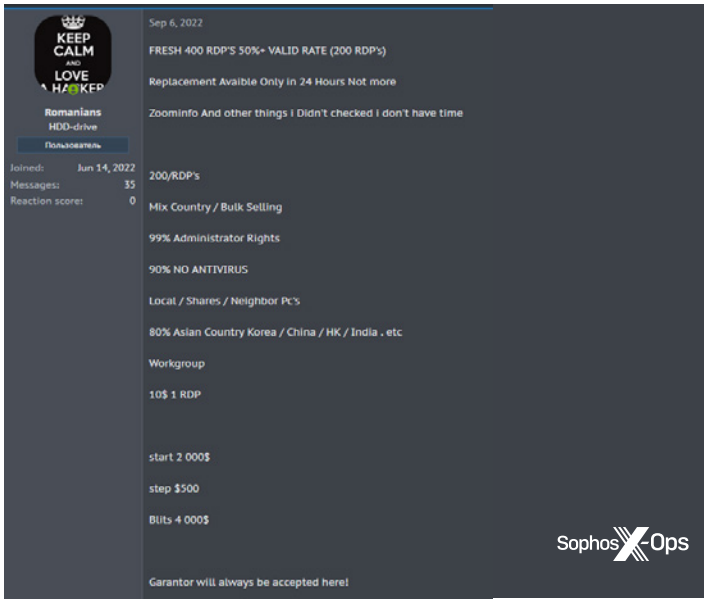

Fig. 3. Un bróker de acceso, buscando una venta rápida, publicita su mercancía.

Fig. 4. Los datos de una empresa de la UE a subasta.

Distribución/propagación de malware como servicio: servicio que facilita la distribución de malware en regiones o sectores específicos, o incluso de forma más generalizada. En los anuncios que vimos para estos servicios, no está exactamente claro cómo se logra esto en cada caso, pero entre los vectores posibles se incluyen los ataques de abrevadero, la explotación de vulnerabilidades o combinaciones con listados de AaaS (acceso como servicio).

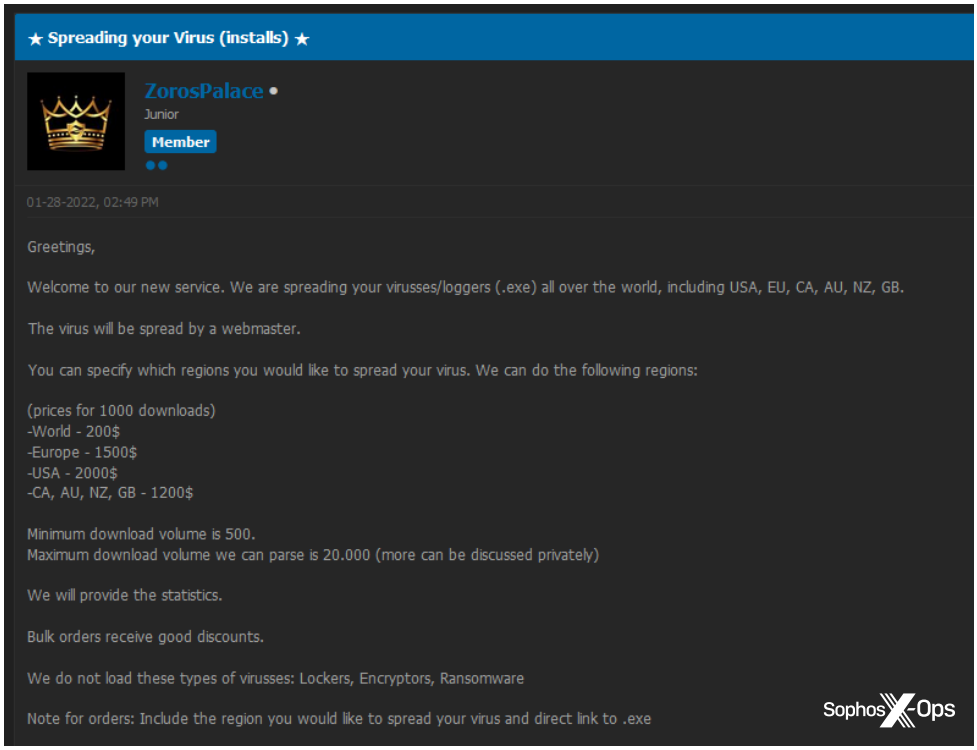

Fig. 5. Un incipiente servicio ofrece servicios de propagación de malware.

Phishing como servicio: oferta de servicios integrales para campañas de phishing, incluyendo sitios clonados, hosting, correos electrónicos diseñados para evitar los filtros de spam y paneles para monitorizar los resultados.

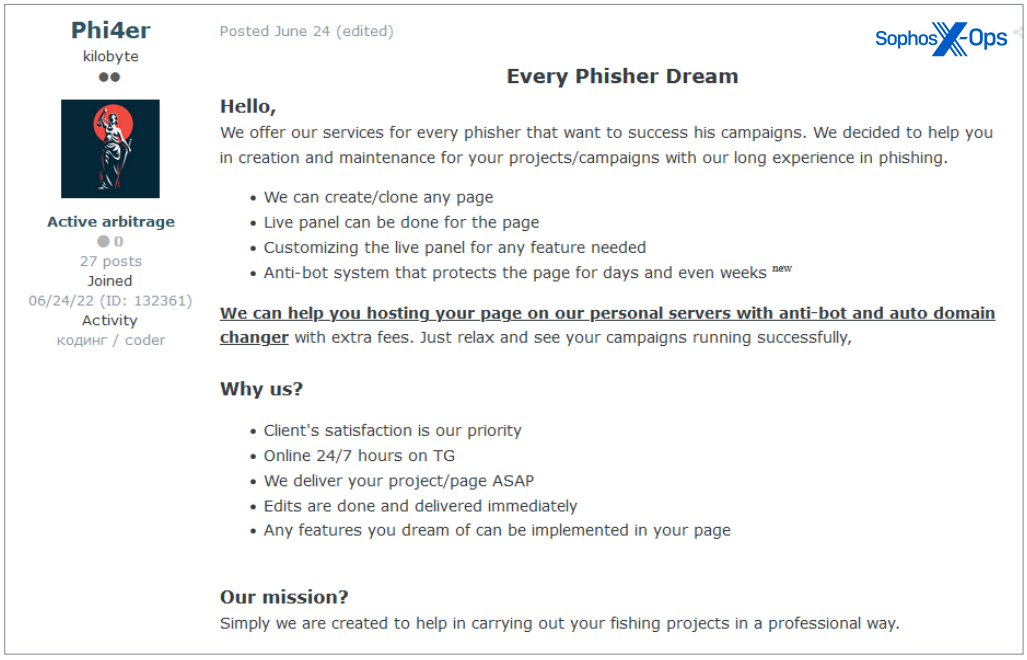

Fig. 6. Un paquete de servicios de phishing con garantías de servicio de atención al cliente incluidas.

OPSEC como servicio: un servicio particularmente interesante, que vimos ofrecido en un paquete con Cobalt Strike en un foro de ciberdelincuentes. El vendedor ofrece asistencia a los compradores proporcionando un servicio OPSEC, bien en forma de configuración única o como suscripción mensual, diseñado para ocultar las infecciones de Cobalt Strike y minimizar el riesgo de detección y atribución.

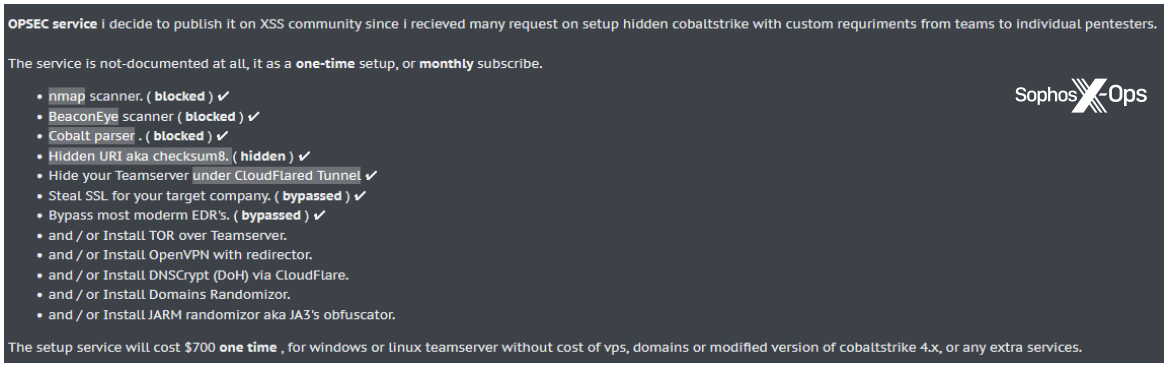

Fig. 7. Proveedores de servicios especiales ayudan a los atacantes a ocultar sus huellas.

Cifrado como servicio: muy servicio común y vendido en muchos foros, el cifrado como servicio está diseñado para cifrar el malware de forma que evite ser detectado, particularmente por Windows Defender y SmartScreen, y en menor medida por productos antivirus. En el ejemplo mostrado a continuación, el servicio se ofrecía por 75 USD para compras puntuales y por 300 USD por una suscripción mensual, que incluía el uso ilimitado del servicio.

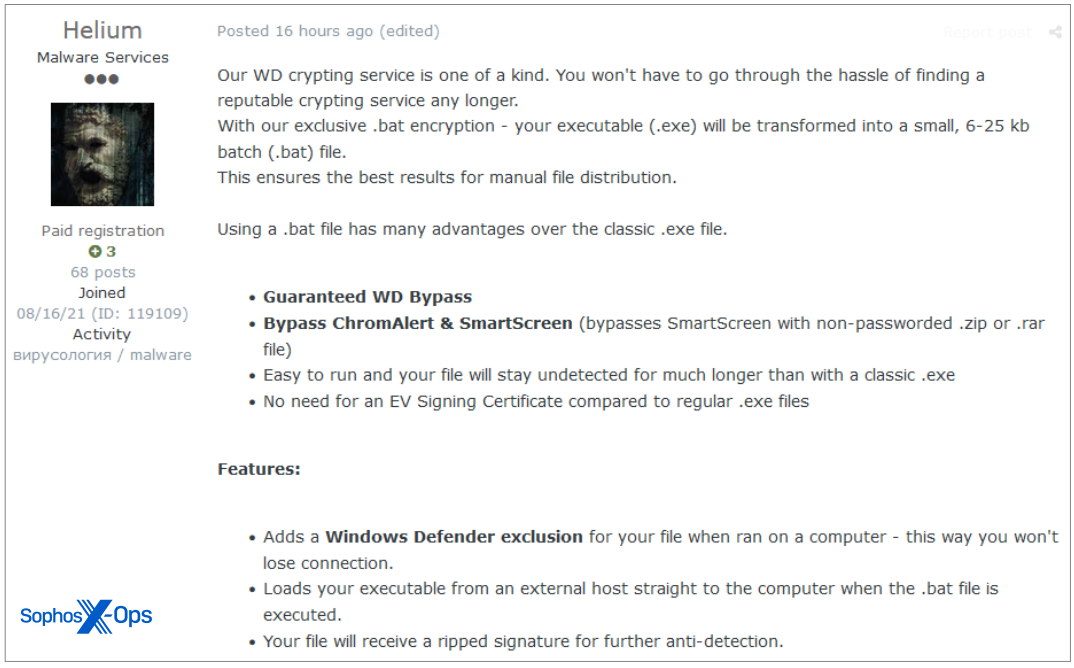

Fig. 8. Para eludir la detección, un servicio especializado ofrece convertir archivos .exe en archivos. bat.

Estafas como servicio: hemos visto unos cuantos ejemplos de «kits de estafas», particularmente relacionados con estafas de criptomonedas, anunciados en foros de delincuentes. No siempre estaba claro lo que se vendía, pero un anuncio ofrecía una «página de estafa sobre Elon Musk regalando BTC» lista para usar por 450 USD. Se trata de una estafa popular por lo menos desde 2018, y ha aparecido varias veces en Twitter, Medium e incluso en un vídeo manipulado con deepfake.

Vishing como servicio: un servicio de phishing por voz («vishing»), mediante el que un atacante ofrecía alquilar un sistema de voz para recibir llamadas junto con un «sistema de IA», de forma que el que lo alquilaba tenía la opción de que sus víctimas hablasen con un bot en lugar de con una persona.

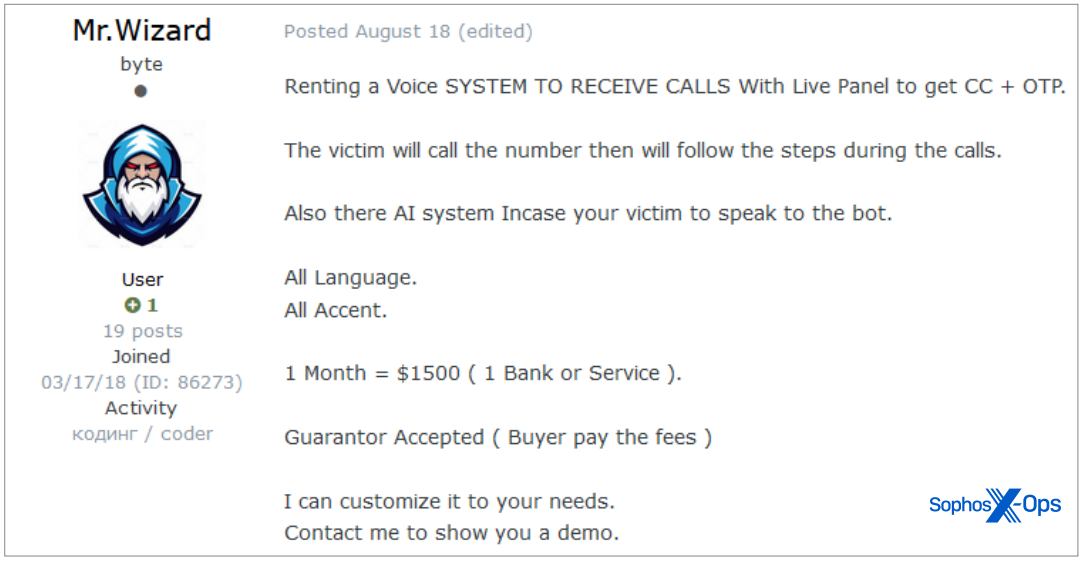

Fig. 9. Una oferta de vishing como servicio incluye «todos los idiomas, todos los acentos».

Spam como servicio: un clásico, pero aún presente en los foros de delincuentes, el spam como servicio ofrece el envío masivo de spam a través de una variedad de mecanismos, incluyendo SMS y el correo electrónico. En algunos casos, el delincuente se ofrece a montar toda la infraestructura desde cero; en otros, la opera y la usa para enviar mensajes de spam personalizados.

Escaneado como servicio: finalmente, un servicio especialmente interesante ofertado en un foro de delincuencia, que ofrecía a los usuarios acceso a un paquete de herramientas comerciales legítimas, incluyendo Metasploit, Invikti, Burp Suite, Cobalt Strike y Brute Ratel, para encontrar (y, presumiblemente, explotar) vulnerabilidades. Como podemos ver en la figura 10, los precios tenían importantes descuentos. Aparentemente, toda la infraestructura es creada y mantenida por el vendedor, que en otra parte especifica que «lo único que hay que hacer es esperar el correo con el resultado del escaneado».

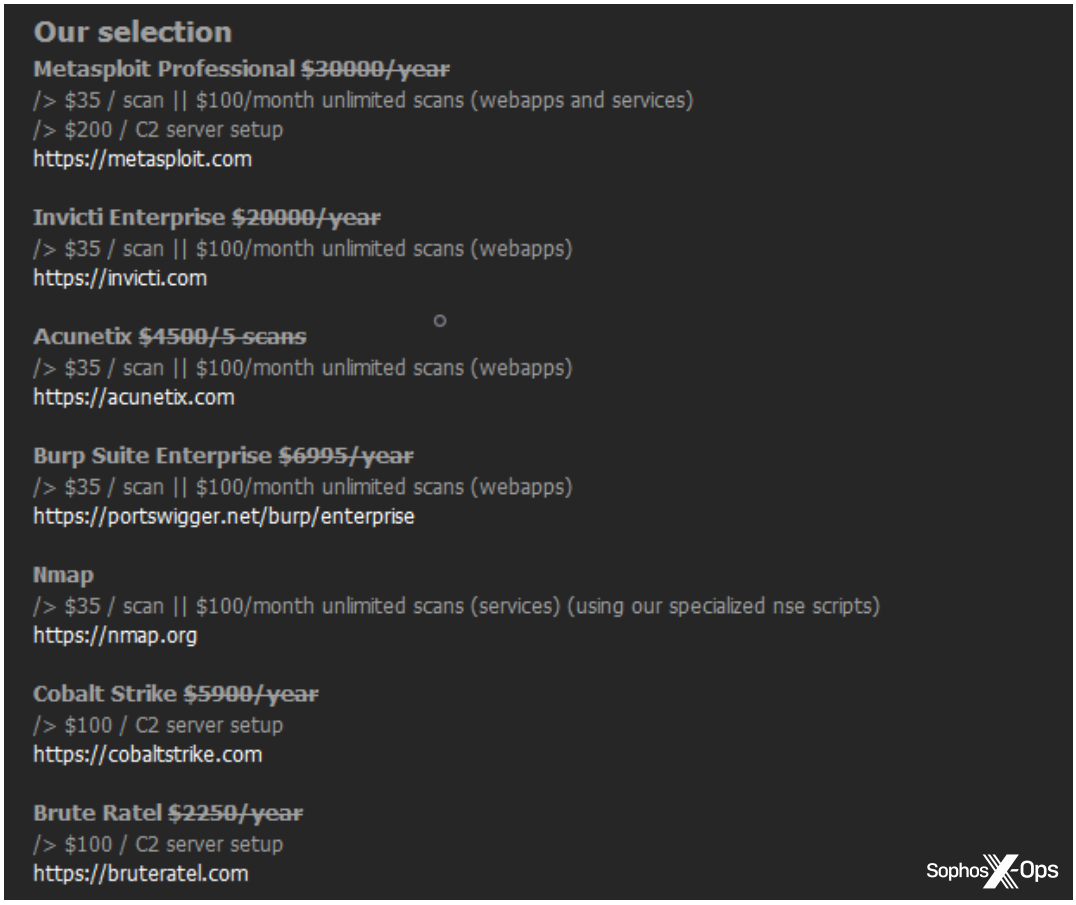

Fig. 10. Un proveedor de escaneado como servicio proporciona un listado con los accesos a distintos paquetes de herramientas comerciales populares.

Evolución hacia una profesionalización sofisticada

A medida que la industria «como servicio» crece, y los mercados ilícitos se convierten cada vez más en mercancías, la imagen y el estilo de estos mercados también cambian. En un foro destacado, por ejemplo, los usuarios pueden pagar por espacio publicitario y mostrar banners animados con anuncios a los miles de usuarios del foro. Obsérvese que uno de los anuncios en el ejemplo a continuación es para el Genesis ya mencionado, un popular mercado que ya hemos tratado.

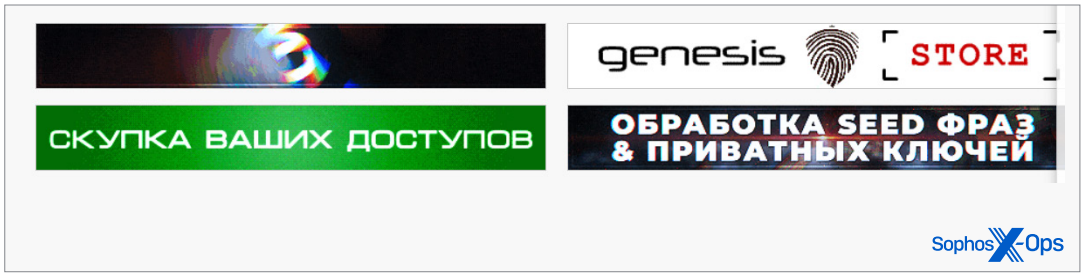

Fig. 11. Un foro de delincuentes muestra anuncios de distintos mercados y servicios.

Los ciberdelincuentes también son cada vez más conscientes de las ventajas de un diseño gráfico y una presentación profesionales. Mientras que hace unos años los listados de malware y servicios solían ser publicaciones sencillas con grandes cantidades de texto que incluían listas de funciones y características, las ofertas de hoy en día suelen ir acompañadas por atractivas imágenes diseñadas para proporcionar a los productos un aire de profesionalidad, diferenciación de marca y legitimidad.

Fig. 12. El servicio Zed Point pretende proporcionar información que podría facilitar la alteración o el robo de identidad.

Fig. 13. NoCryi recopila y mantiene el acceso a cookies de sesión robadas.

En los mercados no solo se anuncian productos y servicios. A medida que la economía delictiva continúa creciendo y profesionalizándose, cada vez es más común encontrar ofertas de trabajo y publicaciones de contratación. Distintos mercados destacados tienen páginas específicas para la búsqueda de colaboradores, tanto para los que buscan empleo (normalmente como «técnicos de pruebas de penetración», frecuentemente un eufemismo para referirse a los afiliados del ransomware), como para los que están contratando personal.

0

[JOB - BTC/XMR] I operate dozens of phishing websites of all kinds. Looking for some "marketers" who can bring people in for a 50/50 split

by **/u/carderman** • 1 week ago in **/d/Jobs4Crypto**

Like the title states, I've got a bunch of different custom-built phishing websites, ranging from fake darknet markets, fake crypto exchanges, email templates with fake giveaways & crypto promos, fake carding sites, simple landing pages, and so on.

I'm looking for someone or someones who'd like to bring people in, via spamming, social engineering, whatever method works for you... and if they take the bait, we split their generous donations 50/50.

I've had some of these up for anywhere from over a year to some I just created this week. These sites bring in a decent chunk of change as they are, but I've never been opposed to more money.

If interested in getting started, or simply learning more about them, just DM me and I can send you some links and you can choose which ones you think you might be able to do something with.

We can keep track of which ones are yours using a coupon code or custom "referral" url. I have a couple ideas for making sure we're on the same page when it comes to keeping track of which "sales" are yours. I'm keen to ensure you're compensated fairly for the hits you bring in because that's just good business - this shit is already passive AF and basically free money for me at the end of the day. But If you can bring in more free money then I'm more than happy to keep you happy if that means you'll keep selling.

Hell, if you're really good, I'd be more than happy to give you the lions share.

Let's make some money, ladies!

SophosX-Ops

Fig. 14. Las alianzas entre entidades con distintas capacidades permite aumentar la eficiencia.

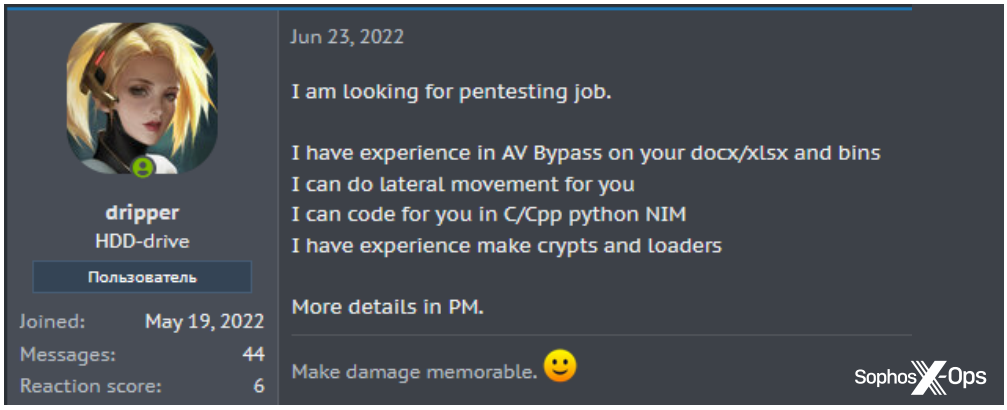

Fig. 15. Un «técnico de pruebas de penetración» experimentado busca trabajo en una entidad establecida.

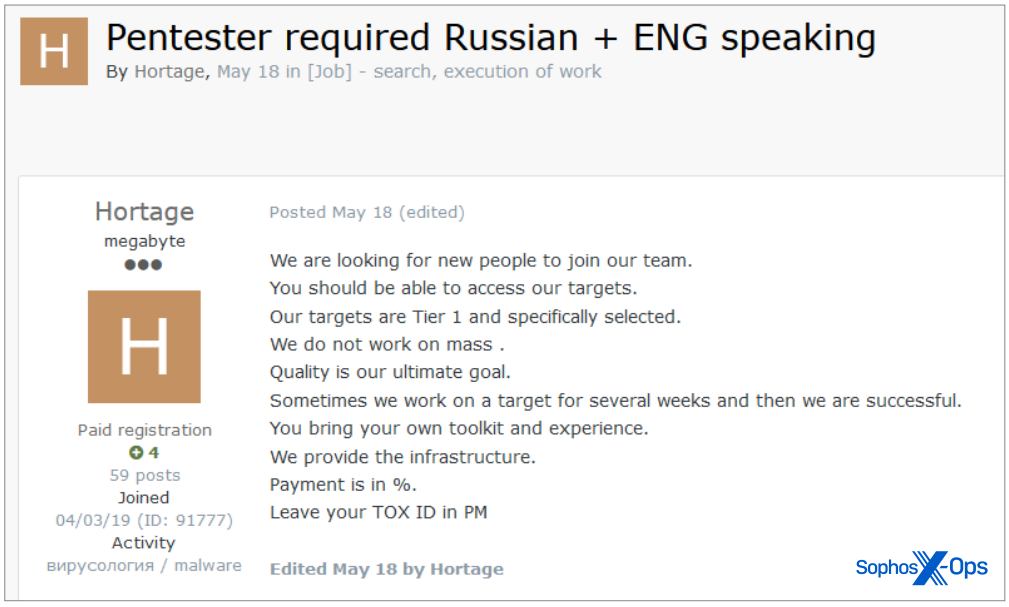

Fig. 16. Una banda de delincuentes establecida busca miembros adicionales.

Ladrones de información

Los servicios de robo de información forman parte de la infraestructura que apoya la economía del malware; son parecidos, pero más extendidos, que las opciones de «[elemento malicioso] como servicio» que acabamos de enumerar. Gracias a las ofertas de malware como servicio y de despliegue de malware como servicio, los ciberdelincuentes en ciernes pueden comenzar con una pequeña inversión y sin grandes conocimientos salvo los necesarios para iniciar sesión en paneles de control web y acceder a mercados de credenciales.

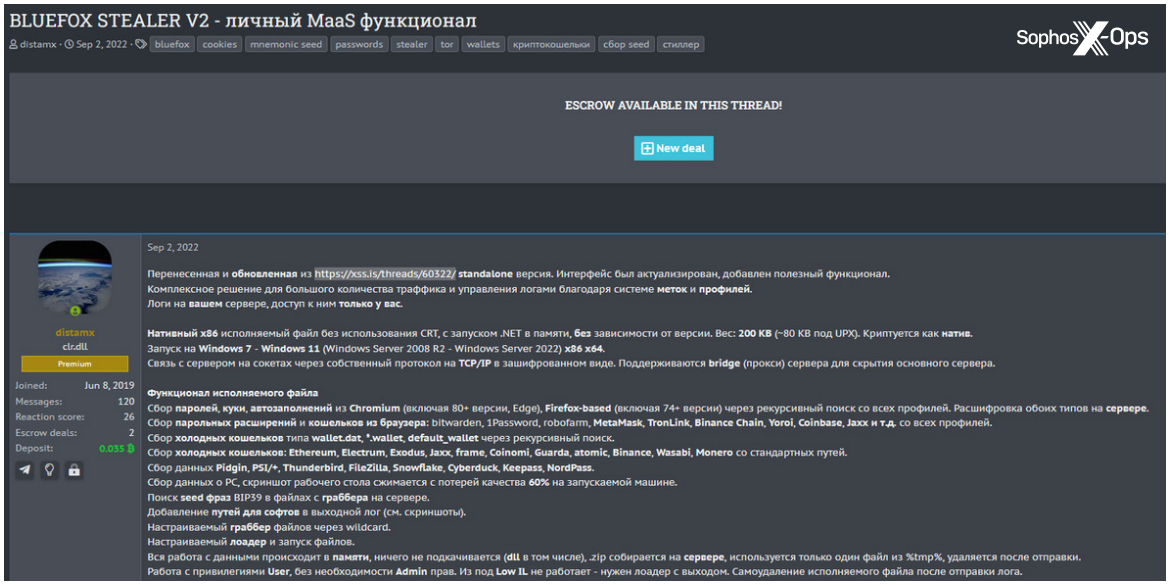

Fig. 17. Los servicios de robo de información prosperan en el ecosistema de la ciberdelincuencia, lo que favorece la especialización.

El ciberdelincuente emprendedor puede entonces revender las credenciales robadas en varios mercados ilícitos. En algunos casos, estas credenciales son meros datos adquiridos incidentalmente, obtenidas en las transacciones de criptodivisas robadas y otros métodos de monetización del malware.

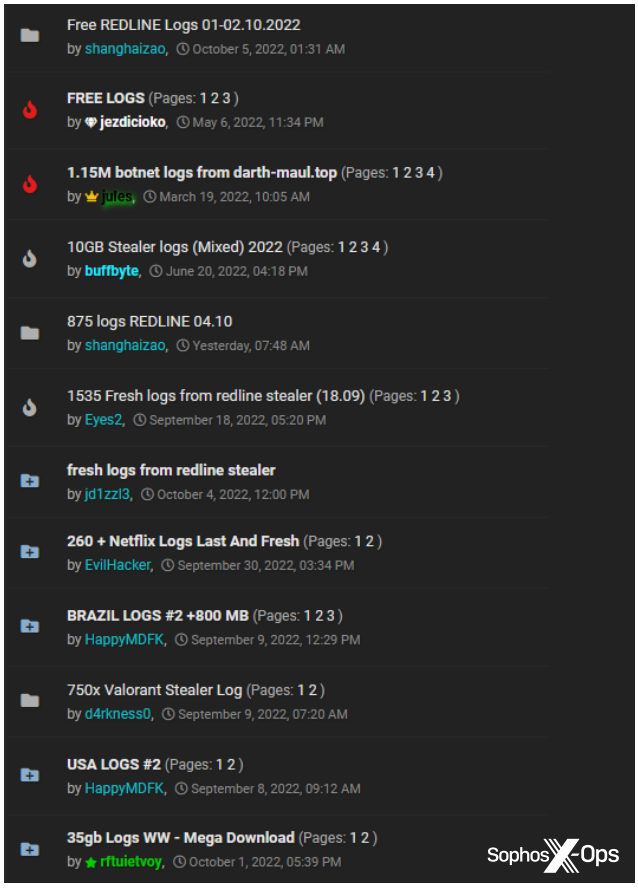

Fig. 18. «Registros» robados, incluidas contraseñas y otras credenciales, a la venta.

Finalmente, el ecosistema de los ladrones de información es muy consciente de que los responsables de la seguridad se interesan por sus acciones, y, como no podía ser de otro modo, ve una oportunidad para sacar provecho. Un foro clandestino, XSS, recientemente trató de monetizar los esfuerzos de los hackers de sombrero blanco para extraer información de sus foros ofertando una suscripción anual de acceso ilimitado para la recopilación de datos por 2000 USD.

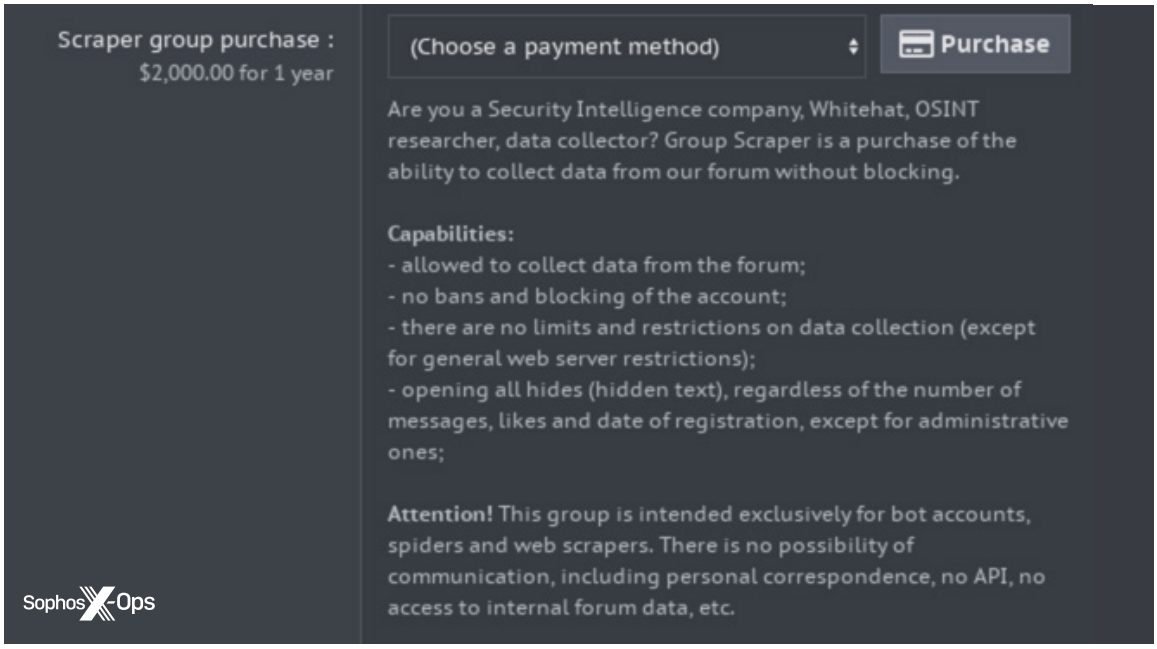

Fig. 19. Un foro ofrece acceso de pago a scrapers de sombrero azul cuyo objetivo es vigilar las actividades delictivas. (La segunda imagen proporciona el texto traducido del ruso al inglés.)

La etiqueta de malware para robar información es muy amplia. Incluye distintos tipos de malware ya tratados en otras partes de este informe, como herramientas de acceso remoto (RAT), registradores de pulsaciones, «clippers» centrados en criptomonedas, y otro malware que sustrae credenciales, cookies de navegadores, transacciones de criptomonedas o cualquier otro dato que pueda robarse rápidamente y venderse o reutilizarse para otros fines maliciosos.

Unos ladrones de información proporcionaron las cookies de Slack utilizadas por la banda Lapsus$ para obtener acceso a la red corporativa de Electronic Arts en 2021. De la misma forma han estado implicados en otras actividades maliciosas más recientes que han aprovechado tokens de sesión para aplicaciones web robados a fin de lograr un acceso más persistente y generalizado, que iba desde estafas por correo electrónico corporativo comprometido hasta ataques de ransomware.

Ladrones de información registrados por porcentaje de equipos únicos

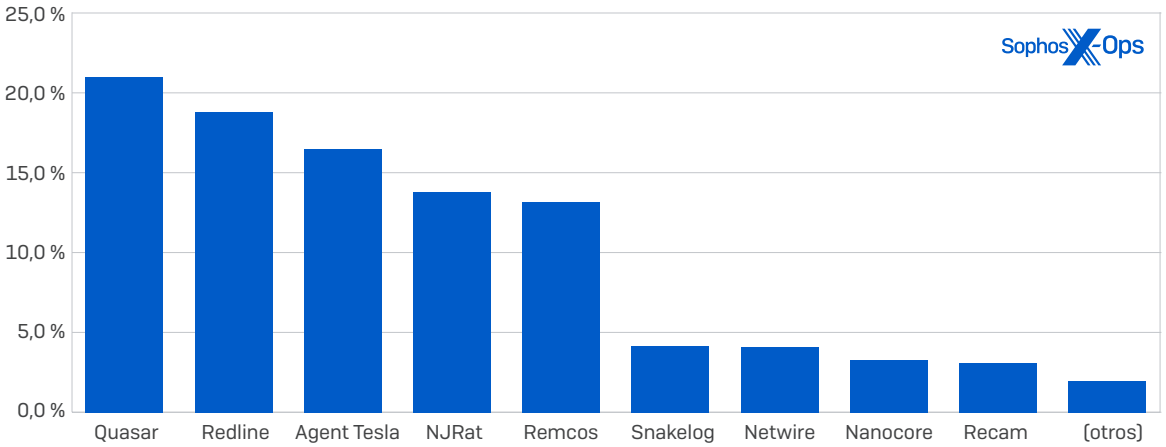

Fig. 20. Quasar, Redline y Agent Tesla representan la mayor parte del malware para robar información descubierto; Quasar se detectó en más de una quinta parte de los equipos infectados durante un periodo de seis meses.

Quienes estén especialmente interesados en los ladrones de información posiblemente hayan observado en el gráfico anterior la ausencia del conocido Raccoon Stealer. Después de aparecer en escena en 2019, el malware basado en Ucrania y centrado en Windows desapareció del panorama temporalmente a inicios de 2022 tras la intervención del FBI en colaboración con las autoridades holandesas e italianas, solo para volver bajo un nuevo mando más adelante ese mismo año. El desarrollo de una nueva versión comenzó en junio, y su finalización se anunció en septiembre en el canal de Telegram de sus autores. Sin embargo, a pesar de la amplia difusión de su relanzamiento, hasta ahora hemos visto pocos casos recientes del nuevo Raccoon Stealer. A finales de octubre, el Departamento de Justicia de los Estados Unidos presentó cargos contra un nacional ucraniano, actualmente bajo custodia de las autoridades holandesas, por conspiración para operar el servicio.

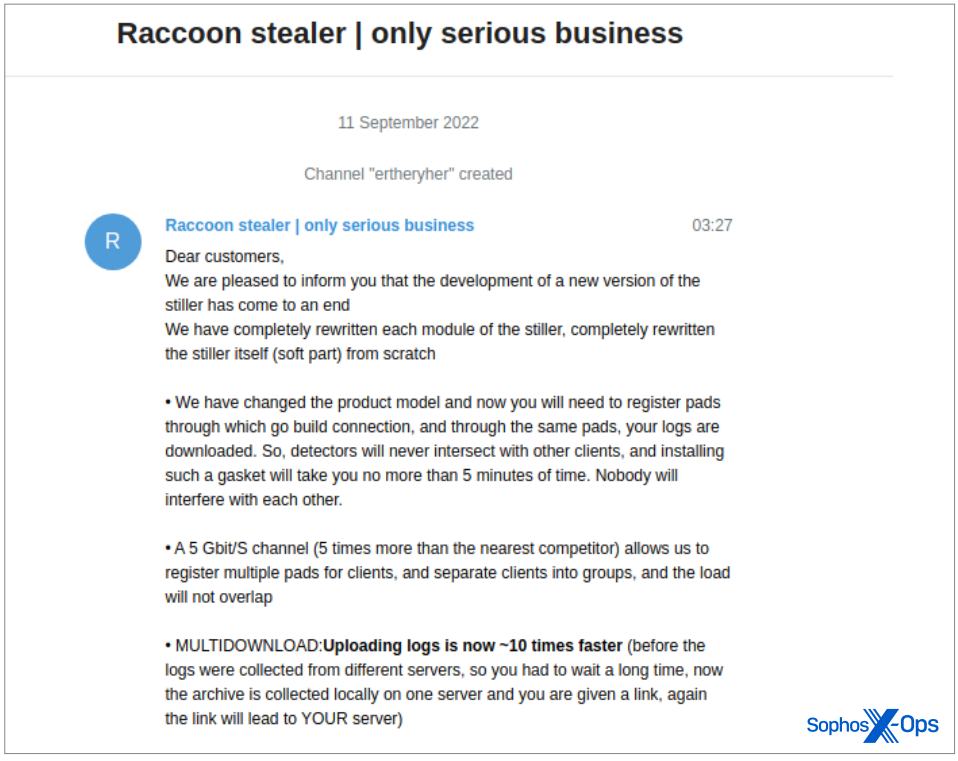

Fig. 21. Raccoon Stealer anunció su última versión en el canal de Telegram del grupo en septiembre.

Los ladrones de información se propagan a través de múltiples canales. Uno de los más comunes son las ofertas de descargadores como servicio basadas en ingeniería social, que incitan a los usuarios a descargar archivos o imágenes de disco que supuestamente contienen instaladores de software legítimos, normalmente anunciados como versiones «crackeadas» que evitan los esquemas de licencias. Las descargas también incluyen instaladores de múltiples paquetes de malware. Estos sitios de descargas utilizan técnicas de optimización para los motores de búsqueda para quedar entre los primeros resultados de cualquier búsqueda de software «crackeado». Otra forma de distribución de pago se produce por medio de redes de bots como Emotet o Qakbot/Qbot.

Algunos ladrones, como Agent Tesla, normalmente utilizan unos enfoques más concretos, creando correos electrónicos maliciosos dirigidos a un grupo específico de víctimas. Estos contienen adjuntos camuflados como documentos urgentes, que en realidad son instaladores de malware.

Pero los ladrones de información se pueden desplegar de formas todavía más específicas. Sophos ha detectado incidentes en los que los intrusos en una red habían utilizado una puerta trasera desplegada a través de Cobalt Strike para ejecutar malware de robo de cookies y otro malware que roba credenciales desde la misma red. Se hicieron esfuerzos para recopilar cookies de navegador desde sistemas que incluían un servidor. Estos entonces se podían usar para obtener acceso como usuarios legítimos a los recursos basados en la web de la organización para subsiguientes propagaciones laterales.

Sophos ha implementado una serie de medidas para bloquear a los ladrones de información y ha añadido una protección contra el robo de cookies para prevenir que los ladrones de información puedan recopilar cookies de sesión.

Evolución del ransomware

Aunque en el último año los grupos de ransomware se han visto algo desarticulados gracias (entre otras razones) a la inestabilidad geopolítica y algún que otro enjuiciamiento, han aparecido nuevos grupos a partir de los viejos, y la actividad del ransomware sigue siendo para las organizaciones una de las amenazas ciberdelictivas más generalizadas. Los operadores del ransomware siguen evolucionando sus actividades y mecanismos, tanto para eludir la detección como para incorporar nuevas técnicas.

Algunos grupos de ransomware han adoptado el uso de nuevos lenguajes de programación en un intento de dificultar más la detección, hacer que el ejecutable de ransomware sea más fácil de compilar para ejecutarse en distintos sistemas operativos o plataformas, o sencillamente porque la gente que desarrolla las cargas de malware es la que utiliza esos conocimientos y herramientas. El lenguaje de programación Rust ha sido adoptado por los desarrolladores del ransomware BlackCat y Hive, mientras que el malware de BlackByte está escrito en Go (también conocido como GoLang).

El ransomware más frecuente en las intervenciones de Sophos Rapid Response durante los primeros diez meses de 2022 ha sido LockBit, seguido de cerca por BlackCat y Phobos. (Sin embargo, reseñamos que el apartado de «otros» representa más de una quinta parte de las familias indicadas, lo que refleja que el panorama del ransomware no se limita en absoluto a unas pocas familias de alto perfil.) La distribución probablemente esté bastante cerca de la distribución global real de los ataques de ransomware en el mundo en general.

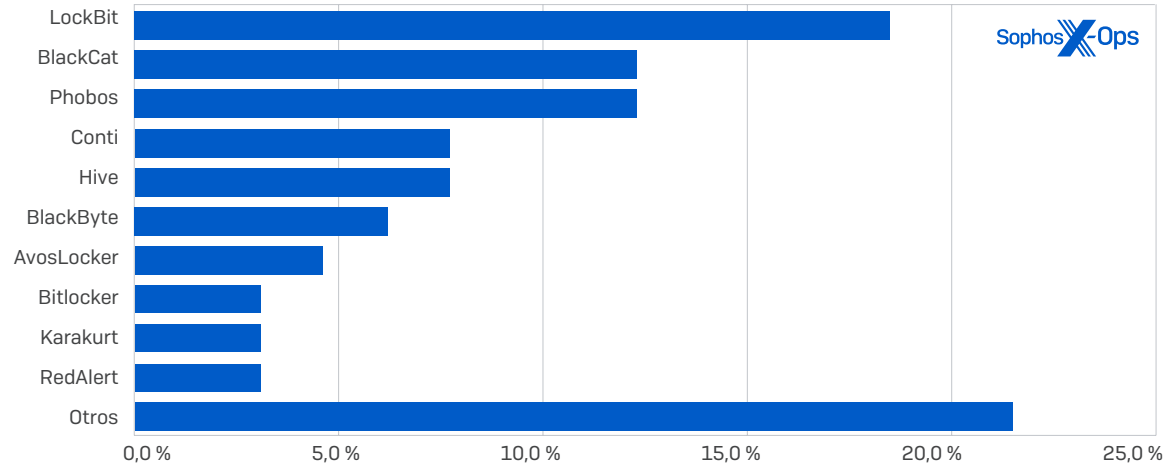

Fig. 22. Entidades de perfil alto como LockBit, BlackCat y Phobos son comunes, pero el panorama observado por Response es sumamente diverso.

Además de usar más idiomas, el ransomware también ha diversificado sus objetivos, no centrándose ya solo en Windows. RedAlert, o N13V, cifra tanto servidores ESXi Windows como Linux, al igual que Luna (otra variante de ransomware basada en Rust). Pero no solo los delincuentes «de segunda» adoptan esta estrategia: los investigadores detectaron una variante de LockBit para Linux-ESXi a comienzos de este año. Los cambios en las plataformas objetivo significan más oportunidades para los atacantes, una mayor superficie de ataque, más presión sobre las víctimas y potencialmente un menor riesgo de detección, ya que la mayoría de las medidas contra el ransomware están centradas en Windows. Veremos más detenidamente los panoramas de amenazas para Linux, Mac y las plataformas móviles más adelante en este informe.

También hemos visto algunos cambios en cómo el ransomware se despliega en los sistemas comprometidos. Dos incidentes de ransomware que nuestro equipo de SophosLabs analizó a principios de año, uno relacionado con el ransomware Darkside y el otro con el ransomware Exx, implicaban el uso malintencionado de aplicaciones normalmente benignas para la carga lateral de DLL. En el caso de Darkside, el atacante utilizó un programa antivirus limpio, mientras que con Exx fue un actualizador de Google. Tras años de popularidad entre determinados atacantes con objetivos especiales, la carga lateral de DLL se está convirtiendo rápidamente en una táctica popular entre los ciberdelincuentes, ya que les permite evadir la detección ejecutando cargas maliciosas bajo la apariencia de procesos legítimos.

En lo que se refiere a la distribución y la propagación del ransomware, los atacantes continúan improvisando y adaptándose. Hemos visto cómo Impacket, una colección de módulos Python de código abierto para trabajar con protocolos de red, se ha aprovechado para la propagación lateral en redes comprometidas. El conjunto de herramientas de Impacket incluye funciones de ejecución remota, rastreo de credenciales y scripts de volcado, exploits para vulnerabilidades conocidas y módulos de enumeración, convirtiéndolo en un paquete muy atractivo para los ciberdelincuentes que usan ransomware. Pretende ser

una herramienta de pruebas de seguridad legítima, pero a semejanza de Metasploit y Cobalt Strike, contiene funciones y características que atraen a clientes menos agradables. En la misma línea, también hemos visto el uso de Brute Ratel para la entrega de cargas, tal como se ha indicado anteriormente. El aumento del uso malintencionado por parte de los atacantes de herramientas de seguridad legítimas («doble uso») requiere que los responsables de la seguridad sean escrupulosamente conscientes de qué está operando en su red (y por qué), y de quién tiene los derechos para hacerlo.

También parece que los grupos de ransomware están explorando oportunidades más generales para diversificar sus operaciones. Un ejemplo clave es el crecimiento de los sitios de filtraciones (leak sites), en los que los atacantes publican detalles de sus víctimas. Tradicionalmente, el modelo ha sido bastante sencillo: si las organizaciones pagan, sus datos no son publicados en el sitio de filtraciones. En caso contrario, sí se publican. Pero este año se han visto algunos desarrollos interesantes en esta materia.

Siendo uno de los grupos de ransomware más importantes, LockBit ha estado por delante de los demás en este aspecto. Su nuevo sitio de filtraciones, en línea con la nueva versión de su ransomware, LockBit 3.0 (también conocido como LockBit Black, posiblemente porque muchas de sus funciones y una parte importante de su código parecen estar basados en el ransomware BlackMatter), contiene algunas funciones novedosas. Por ejemplo, un método para ganar dinero diseñado por el grupo es ofrecer a los visitantes, o a la víctima, la posibilidad de destruir o comprar los datos robados, o de ampliar la cuenta atrás para la publicación.

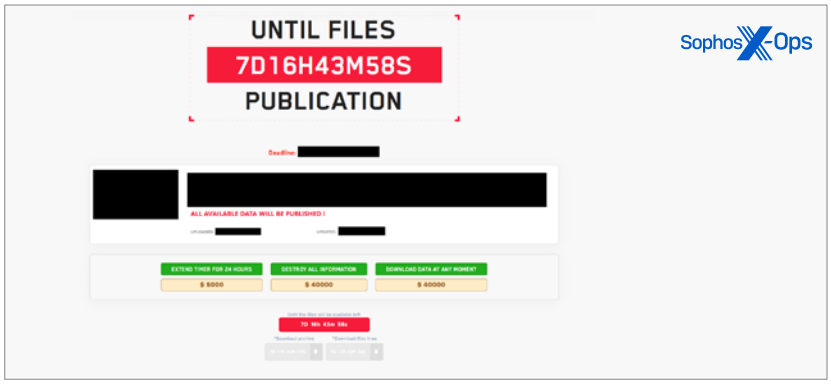

Fig. 23. A la víctima de LockBit se le presenta la opción de ampliar la cuenta atrás del ransomware o descargar (o destruir) los datos.

Otros grupos de ransomware, como Karakurt y AvosLocker, se han subido a este carro, organizando subastas de los datos robados. Otros, como Snatch, incluso prometen pasar sus filtraciones a un modelo de suscripción. Algunos sitios ofrecen una vuelta de tuerca más a la visibilidad posterior a la divulgación: si una víctima paga, no solo no se hace pública la información, sino que tampoco se hace público el hecho en sí de la filtración (o si la situación de la víctima se ha publicado en sitios de filtraciones, esa mención se elimina). Posiblemente esto convierte a la víctima en cómplice de la ocultación de una actividad que en muchos países es obligatorio comunicar a las autoridades.

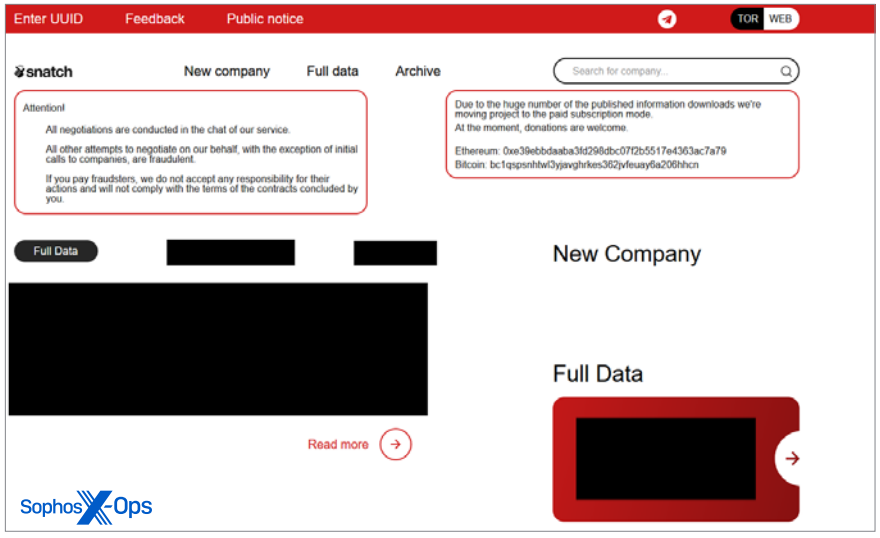

Fig. 24. El ransomware Snatch cambia a un modelo de suscripción.

Pero LockBit ha dado un paso más, al innovar no solo en lo que respecta a su producto principal, sino también en sus interacciones y su posición dentro de la comunidad delictiva. Así, su nuevo sitio de filtraciones, por ejemplo, ofrece un programa de recompensas por la detección de errores, con remuneraciones «desde 1000 USD a 1 millón USD», ofrecidas por actividades que, en última instancia, reforzarían el servicio:

- Revelación en privado de fallos en su página web o malware.
- Un doxing exitoso de la persona al mando del propio programa de afiliados de LockBit, con detalles de cómo se ha logrado, presumiblemente para que LockBit pueda reforzar su OPSEC (esta es la recompensa del millón de dólares).
- Vulnerabilidades en la mensajería TOX (un paquete de mensajería instantánea usada de forma importante por los ciberdelincuentes).
- Ideas para mejorar el ransomware de LockBit.
- Vulnerabilidades en términos de revelación de información en su dominio .onion u otros aspectos de la red TOR.

LockBit no es la primera banda de ciberdelincuentes en ofrecer programas de recompensas por identificar fallos. En noviembre de 2021, All World Cards, un destacado grupo de carding activo en distintos foros de ciberdelincuencia en ruso ofrecía recompensas de hasta 10 000 USD por encontrar vulnerabilidades en su tienda. Y probablemente no sea la última. Es una forma efectiva de externalizar las pruebas de penetración y las evaluaciones de vulnerabilidades, a la vez que se asegura que los resultados se queden entre el investigador y el atacante.

Fig. 25. All World Cards presentó un modesto programa de recompensas por detectar errores a finales de 2021.

Finalmente, hemos observado unos cuantos grupos de ransomware o filtraciones menos conocidos que, a diferencia de sus primos más famosos, parecen tener motivaciones políticas. En primer lugar se encuentra un sitio de filtraciones dedicado a compartir material de filtraciones robado a organizaciones gubernamentales y ciudadanos ucranianos, aunque no está claro el origen de los datos ni si hay implicado ransomware.

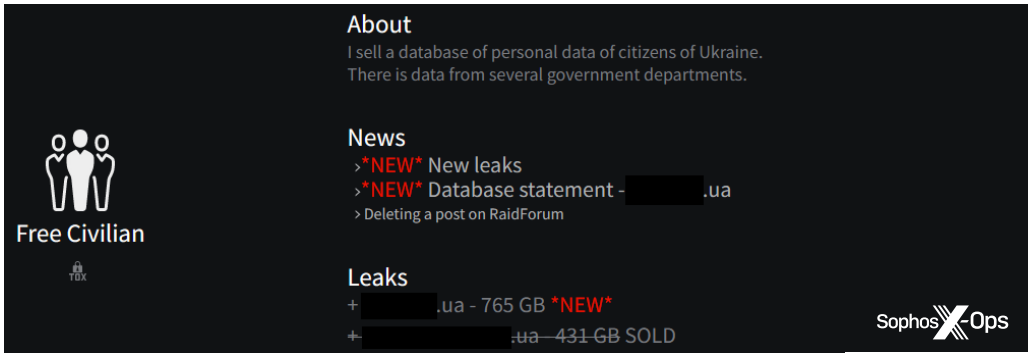

Fig. 26. Civiles ucranianos objetivo de un atacante centrado en ese país.

También hay un grupo conocido como Moses Staff, que parece dirigirse contra organizaciones israelíes con tácticas que se asemejan al ransomware pero sin pedir rescates.

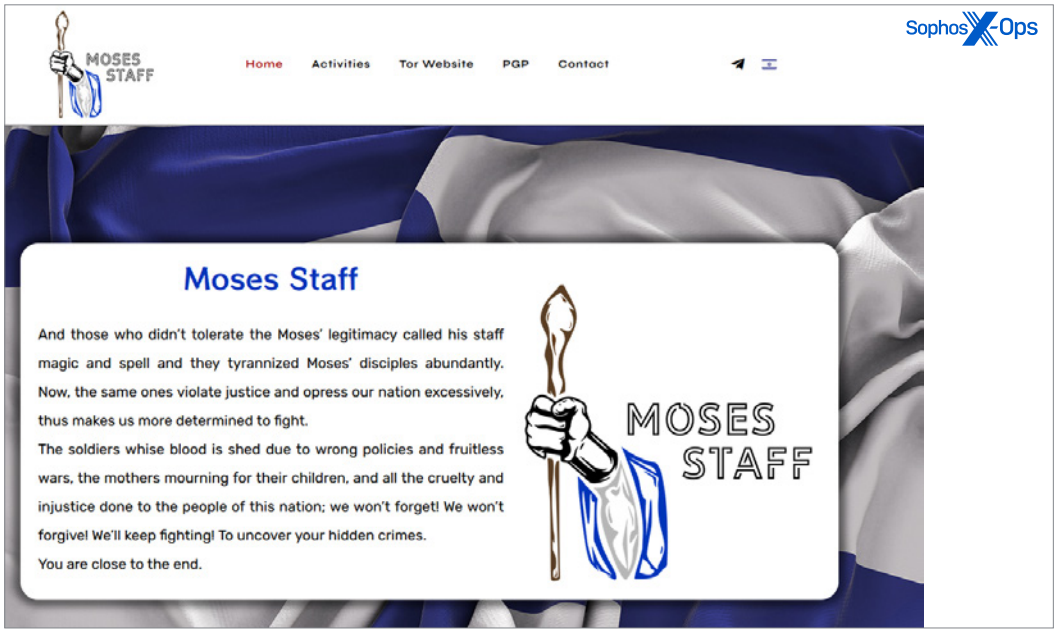

Fig. 27. Grupo antiisraelí utiliza tácticas semejantes al ransomware para acosar.

Herramientas de ataque

Para la mayoría de los responsables de la seguridad, entender «quién» lanzó los ataques es algo menos factible que conocer el «cómo». En esta sección veremos las formas en las que los atacantes manipulan actualmente las herramientas de seguridad ofensiva para lograr sus objetivos. Las herramientas de pruebas de penetración son un candidato obvio para un uso malintencionado, pero no son las únicas herramientas legítimas de seguridad vulneradas. Resumiremos otras técnicas, incluido el uso de las herramientas de acceso remoto (RAT), por lo demás legítimas. A continuación centraremos nuestra atención en el aumento de los «LOLBin», una técnica que se aprovecha de los binarios ya presentes en los sistemas atacados, y al repunte reciente de atacantes que usan controladores y DLL de terceros, normalmente legítimos, para infiltrar código malicioso a través de las defensas. Finalmente, dedicaremos algo de tiempo a dos especies de malware que nos parecieron especialmente interesantes en 2022: el ransomware dirigido contra las actualizaciones de seguridad de endpoints y el software «minero» que roba los recursos de las víctimas para destinarlos a la extracción de criptomonedas. Finalizaremos nuestro informe con un repaso al panorama de amenazas que acechan a Linux, Mac y los dispositivos móviles.

El uso malintencionado de las herramientas de seguridad ofensiva

El uso indebido de herramientas de seguridad ofensiva, es decir, software destinado a ser usado por los equipos de seguridad de la información para simular ataques activos, es algo normal en muchas campañas de ransomware. Como ya observamos el año pasado, copias piratas de la herramienta de pruebas de penetración Cobalt Strike están siendo usadas cada vez más por adversarios como los afiliados de ransomware. Las herramientas de código abierto desarrolladas por la comunidad de seguridad ofensiva siguen siendo el principal componente de las detecciones de herramientas de ataque. Algunos ejemplos incluyen la herramienta de extracción de credenciales Mimikatz (cuyas versiones representan aproximadamente dos quintas partes de las detecciones de herramientas de ataque únicas en la telemetría de Sophos), otras herramientas de explotación basadas en PowerShell, como PowerSploit, y componentes de «Meterpreter» conectados a la plataforma de explotación Metasploit, parcialmente de código abierto.

Pero las copias piratas de herramientas de seguridad ofensiva comerciales se han convertido en un componente estándar de ataques más complejos y profesionales. Como ya hemos documentado más arriba, algunos grupos publican anuncios para contratar personas con experiencia en el uso de estas herramientas. Y las copias piratas de Cobalt Strike y la versión comercial de Metasploit ahora son tan comunes que frecuentemente se publican enlaces a copias gratuitas en sitios clandestinos (aunque algunas pueden ser en realidad malware).

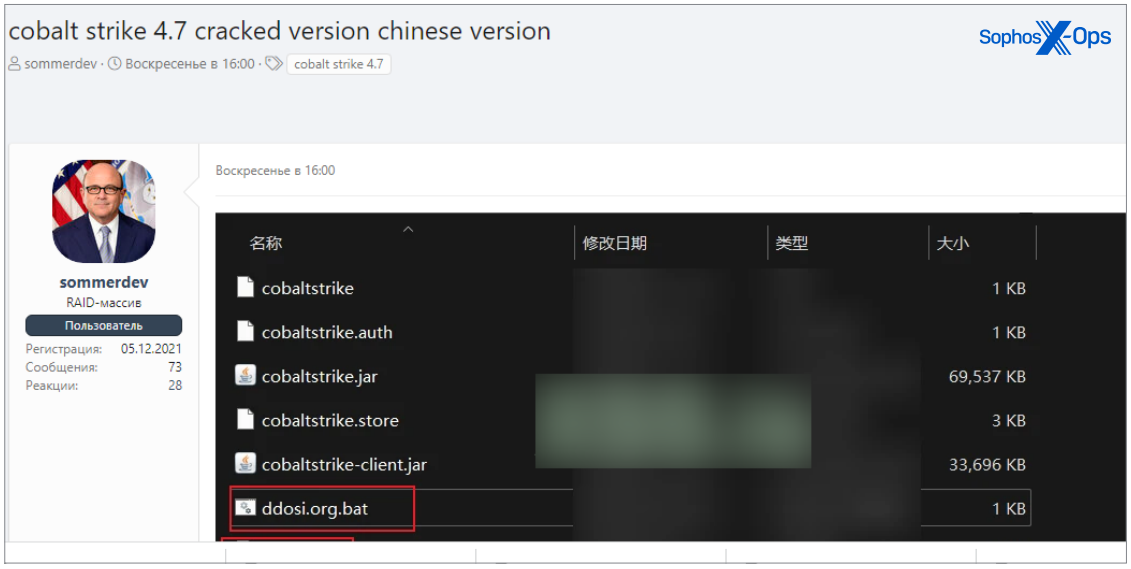

Fig. 28. Reventa de una versión en chino de Cobalt Strike 4.7 crackeada.

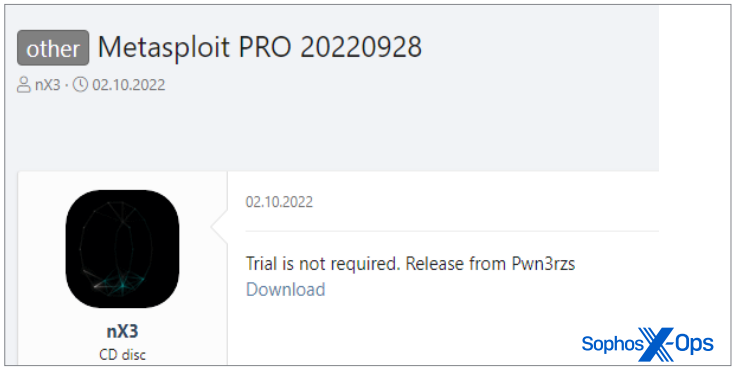

Fig. 29. Versión de pago de Metasploit pirateada y ofrecida para su descarga.

Cobalt Strike estuvo implicado en el 47 % de los incidentes de clientes gestionados por el equipo Sophos Rapid Response durante los tres primeros trimestres de 2022. La gran mayoría de estos estaban relacionados con el ransomware, o eran actividades «previas al ransomware» en las que se detectó que los atacantes utilizaban técnicas, herramientas y prácticas asociadas con ataques de ransomware inminentes. Pero Cobalt Strike también se ha observado en ataques a estados, como en la campaña contra SolarWinds de 2020 y en ataques contra objetivos en Ucrania por parte de hackers alineados con Rusia.

Por sí solo, Cobalt Strike representó el 8 % de todas las detecciones específicas de herramientas de ataque. Además, su protocolo de comunicación se ha implementado en otras herramientas desarrolladas por atacantes. TurtleLoader, por ejemplo, tiene versiones que se conectan a su red de comando y control (C2) mediante el protocolo de conexión de Metasploit o Cobalt Strike. Adversarios como estos, que utilizan múltiples herramientas, constituyen un desafío interesante para los responsables de la seguridad, especialmente porque se emplean distintas capas de defensa como protección contra los ataques.

Y siempre hay más cosas por las que estar alerta. En el momento de redactar este informe, por ejemplo, habíamos visto la subida de los ataques con Brute Ratel, consecuencia de la nueva disponibilidad de este conjunto de herramientas para los atacantes. En el momento de pasar a imprenta, las detecciones de Brute Ratel eran casi insignificantes, con menos del 1 % de nuestras detecciones en memoria. Esto casi seguro cambiará en 2023, a medida que proliferen las versiones pirateadas del producto.

Detecciones de herramientas de ataque destacadas (equipos únicos en un periodo de muestra de 6 meses)		
Herramienta de ataque	**Porcentaje de equipos infectados**	**Notas**
Mimikatz	24,7 %	Utilidad de código abierto de volcado de credenciales posterior a la explotación
Apteryx	14,5 %	Versión compilada de Mimikatz
Paquete PowerSploit	11,7 %	Código abierto; sin soporte oficial desde agosto de 2020
SrpSuite	8,3 %	Paquete PowerShell de código abierto de FuzzySecurity
Cobalt Strike	8,0 %	Software propietario, frecuentemente pirateado/crackeado
Meterpreter	7,8 %	Carga de ataque Metasploit de código abierto; disponible soporte comercial
Nishang	6,8 %	Plataforma y scripts/cargas para usar con PowerShell
TheFatRat	6,2 %	Automatización de puertas traseras/ cargas Metasploit de código abierto
TurtleLoader	5,4 %	Puerta trasera, normalmente vista en combinación con Metasploit o Cobalt Strike
JMeter	5,1 %	Metasploit basado en Java
Juicy Potato	5,0 %	Exploit BITS de código abierto (herramienta de aumento de privilegios)
winPEAS	4,8 %	Scripts de aumento de privilegios y robo de información
Swrort	4,6 %	Puerta trasera basada en Metasploit
Empire	4,5 %	Plataforma posexplotación de código abierto; fusión de PowerShell Empire y Python EmPyre; sin soporte oficial desde julio de 2019

Fig. 30. El porcentaje de los equipos infectados analizados por Sophos en los que estuvo presente la herramienta indicada, junto con información adicional sobre algunas herramientas; datos obtenidos en un periodo de seis meses (abril-septiembre 2022) y omisión de las herramientas detectadas en menos de un 4,5 % de equipos únicos por motivos de espacio.

Hasta septiembre de 2022, el desarrollador de Brute Ratel afirmaba tener un control estrecho sobre el acceso a la herramienta mediante la concesión de licencias. A pesar de ello, parece que atacantes asociados con el grupo de ransomware Conti han creado empresas falsas para adquirir la plataforma, y por lo menos ha habido un caso de filtración de una licencia por un empleado de un cliente legítimo. Desde septiembre en adelante, copias piratas de una versión reciente de Brute Ratel están disponibles de forma generalizada en los mercados clandestinos.

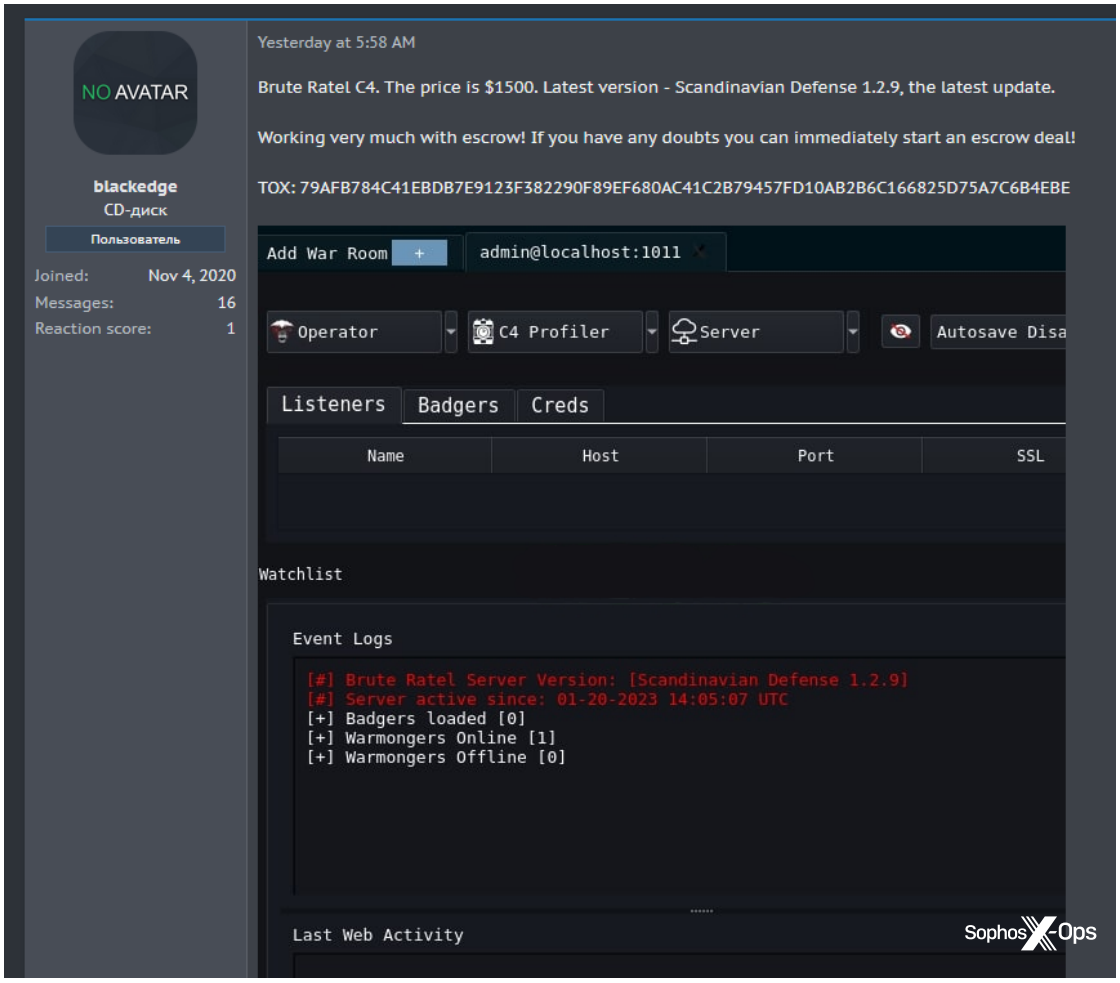

Fig. 31. Una versión crackeada de Brute Ratel debuta en el mercado clandestino.

Hasta ahora, solo hemos documentado algunos ataques asociados con componentes de Brute Ratel. Durante la clasificación de un incidente por Sophos MDR, observamos que los atacantes primero intentaron utilizar Cobalt Strike; cuando se detectó y bloqueó, los adversarios intentaron desplegar Brute Ratel, que también fue bloqueado.

Pero es muy probable que haya más incidentes. Posiblemente como resultado de la disponibilidad más generalizada de Brute Ratel, investigaciones recientes han detectado la propagación de agentes de Brute Ratel por Qakbot, de forma similar a como se han propagado las cargas de Cobalt Strike en el pasado.

Otras herramientas de seguridad usadas de forma malintencionada

Brute Ratel no es el único kit de herramientas que se utiliza con intenciones maliciosas: los ciberdelincuentes también ponen a la venta otras herramientas de seguridad legítimas en los mercados clandestinos. Algunos ejemplos son Core Impact, una plataforma de pruebas de penetración; Nexpose, un escáner de vulnerabilidades; VirusTotal Enterprise; y Carbon Black, una plataforma de protección de endpoints.

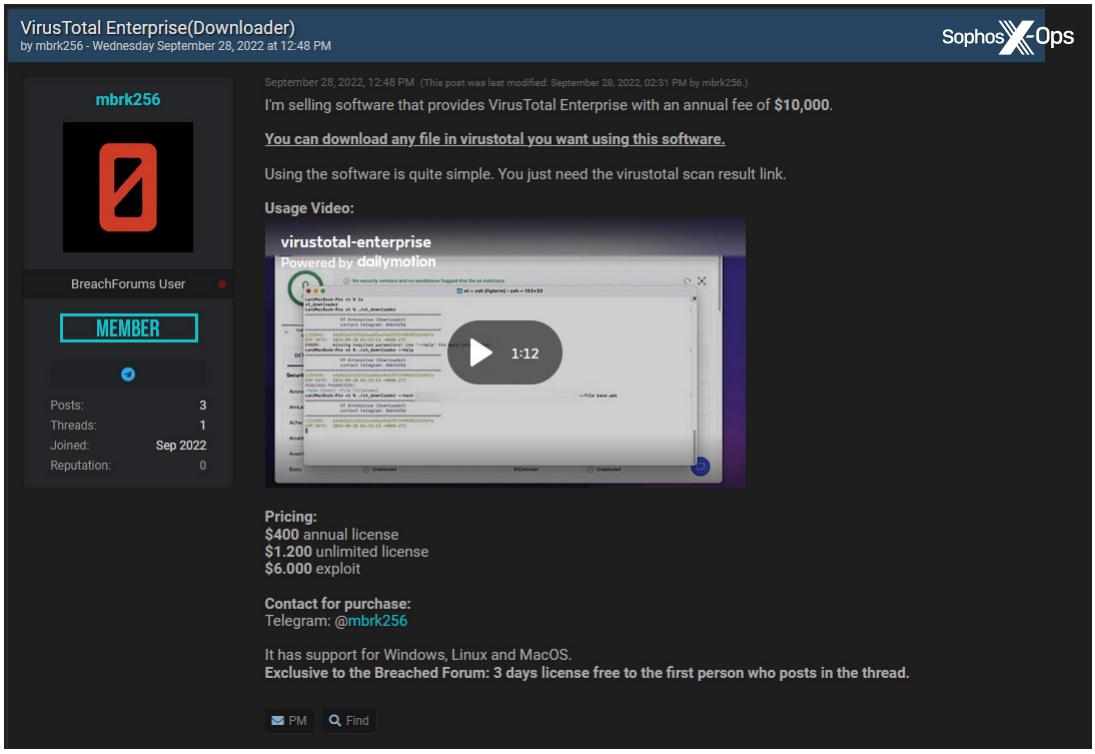

Fig. 32. VirusTotal Enterprise, atacado por scrapers de datos maliciosos.

Los casos de uso de estas herramientas perfectamente legítimas por parte de los ciberdelincuentes varían: pueden diseccionar plataformas de EDR y de protección de endpoints para probar vulnerabilidades y tácticas de evasión; automatizar el escaneado y la explotación de vulnerabilidades con pruebas de penetración y marcos de explotación; y obtener muestras de malware y contrainteligencia con herramientas como Virus Total.

RAT de doble uso

En el conjunto cada vez más amplio de herramientas de seguridad usurpadas o sencillamente usadas de forma malintencionada en el panorama de amenazas, se deben mencionar especialmente las herramientas de acceso remoto. La frecuencia con la que estas herramientas legítimas se usan para fines ilegítimos, un ejemplo tóxico de «doble uso», requiere que los encargados de la seguridad mantengan una vigilancia constante para detectar señales de explotación y comportamientos dudosos.

Las herramientas de acceso remoto se usan para establecer una conexión persistente con sistemas comprometidos desde los cuales orquestar ataques. Algunas de las herramientas de acceso remoto más destacadas son:

- NetSupport Manager (NetSupport)
- TeamViewer Remote Access (TeamViewer)
- ConnectWise Control/Screenconnect Remote Access (ConnectWise)
- AnyDesk (AnyDesk Software)
- Atera (Atera Networks)
- Radmin (Famatech)
- Remote Utilities (Remote Utilities)
- Action1 RMM (Action1)

Estas herramientas pueden ser desplegadas por los propios atacantes, o por brókeres de acceso que venden accesos persistentes a redes comprometidas. Algunos ciberdelincuentes solicitan abiertamente el acceso a los sistemas de las víctimas con estas herramientas en sitios web clandestinos:

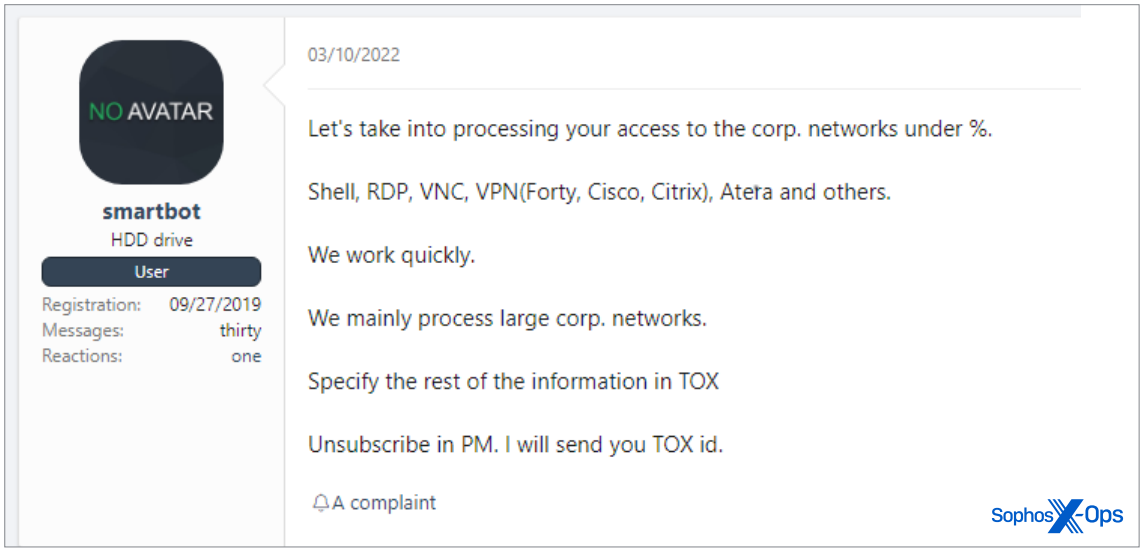

Fig. 33. Oferta de acceso a redes vulneradas a través de herramientas comprometidas.

La herramienta Atera fue detectada como parte integrante de distintos intentos de incursión investigados por Sophos, incluyendo una serie de intentos de distribuir malware aprovechando la vulnerabilidad Log4J, y en distintos casos de ransomware investigados por Sophos Rapid Response. En los intentos de explotación a través de Log4J, centrados en servidores VMWare Horizon, los atacantes trataron de ejecutar un script de PowerShell remoto para descargar e instalar de forma silenciosa el agente de Atera con una licencia de evaluación (junto con otra herramienta de acceso remoto legítima explotada, Splashtop Streamer). En los incidentes observados por Rapid Response, las instalaciones de Atera se habían completado explotando servidores de Microsoft Exchange vulnerables. Y los operadores del ransomware BlackCat han explotado TeamViewer y AnyDesk en incidentes recientes investigados por Rapid Response.

En muchos casos, el uso malintencionado de estas herramientas legítimas puede detectarse y bloquearse basándose en contextos anómalos, como eventos de instalación extraños (por ejemplo, una versión de NetSupport instalada por PowerShell en un directorio distinto al normal). Además, el uso indebido de estas herramientas puede ser detectado en algunos casos por el uso de una licencia de evaluación para el despliegue. Sophos ha desplegado reglas de comportamiento que detectan el uso malintencionado de la licencia de evaluación de Atera y continúa desarrollando técnicas de detección de comportamientos para el uso indebido de este y otros paquetes de acceso remoto.

Binarios LOLBin y ejecutables legítimos

Una característica importante de los ataques de adversarios activos, así como de algunos ataques más automatizados, es el uso de «binarios que viven de la tierra», o LOLBin. Estos componentes nativos de Windows son aprovechados por los ciberdelincuentes para ejecutar comandos del sistema, evadir funciones de seguridad predeterminadas, descargar y ejecutar archivos maliciosos remotos y propagarse lateralmente por las redes.

El principal LOLBin, la shell de comandos de Windows (cmd.exe), es utilizado por la mayoría de puertas traseras y shells para ejecutar comandos del sistema y lanzar malware, de forma que está presente de alguna forma prácticamente en cualquier ataque de malware. Cada una de las plataformas de scripting de Windows –PowerShell, Microsoft HTML Application Host (mshta.exe) y Windows Scripting Host (wscript.exe)– son usadas como herramientas para ejecutar llamadas a la API de Windows, descargar y ejecutar otro contenido malicioso, ejecutar comandos del sistema y recopilar datos. Adicionalmente, PowerShell es usada por muchas de las herramientas de ataque utilizadas por los ciberdelincuentes.

Otro componente de Windows usado de forma ilícita con frecuencia, rundll32.exe, suele ser utilizado por los operadores de ransomware para cargar malware en formato de biblioteca de enlaces dinámicos (DLL). Pero hay otros ejecutables legítimos y firmados que pueden ser explotados de forma similar e intervenir en tareas de ejecución de puertas traseras o ransomware.

Otros LOLBin no son tan obvios. La utilidad de certificados de Windows (certutil.exe), que puede recuperar contenido de servidores web remotos, frecuentemente es explotada por operadores de ransomware y otros ciberdelincuentes para descargar y descodificar archivos maliciosos. Bitsadmin.exe, la utilidad de línea de comandos para el Servicio de transferencia inteligente en segundo plano, se utiliza para mover archivos hacia, desde y dentro de una red objetivo sin que el proceso que inició la transferencia tenga que permanecer activo, lo que la convierte en ideal para la propagación lateral de malware o la exfiltración de datos.

Este tipo de comportamiento puede detectarse y bloquearse de distintas formas. El comportamiento malicioso que usa PowerShell y otros motores de scripting puede detectarse monitorizando la Interfaz de análisis antimalware (AMSI) de Windows. El análisis comportamental de la ejecución de LOLBin a través de llamadas al sistema o desde una línea de comandos también puede detectar este uso malintencionado.

Los diez principales LOLBin por porcentaje de equipos afectados		
LOLBin	**Porcentaje de detecciones no procesadas**	**Notas**
cmd	92,26 %	Intérprete de comandos por defecto
powershell	1,79 %	Línea de comandos y shell de scripting más avanzadas
certutil	1,09 %	Programa de línea de comandos instalado como parte de los servicios de certificados
mshta	1,01 %	Microsoft HTML Application Host, permite la ejecución de .HTA (aplicación HTML)
bitsadmit	0,95 %	Servicio de transferencia inteligente en segundo plano, utilizado como parte de las actualizaciones de Windows para la transferencia de archivos
wscript	0,93 %	Windows Scripting Host compatible con la ejecución de JScript y VBScript
bcdedit	0,83 %	Herramienta de línea de comandos para gestionar los datos de la configuración de arranque
rundll32	0,52 %	Se utiliza para cargar y ejecutar bibliotecas de enlaces dinámicos de 32 bits (DLL)
nltest	0,39 %	Herramienta que proporciona información de diagnóstico
ProcDump	0,21 %	Aplicación de línea de comandos que proporciona información sobre los procesos del sistema

Fig. 34. El omnipresente cmd.exe es, de lejos, el objetivo general más común para el uso malintencionado de LOLBin en sistemas Windows (abril-septiembre 2022).

Sophos X-Ops

Vulnerabilidades «propias»

Aparte de los LOLBin, otros ejecutables legítimos se utilizan a menudo como parte de ataques de ransomware y otros ciberdelitos. En este caso, las aplicaciones son aportadas por el atacante. En algunos casos, se trata de ejecutables vulnerables que pueden usarse para la carga lateral de código malicioso. Este fue el caso de un componente obsoleto firmado por McAfee usado en un ataque de ransomware AtomSilo el año pasado para desplegar una puerta trasera de Cobalt Strike.

Otra versión de este método es la técnica «Bring Your Own Vulnerable Driver» (traiga su propio controlador vulnerable), que aprovecha un controlador legítimo y firmado con una vulnerabilidad explotable para obtener un acceso de bajo nivel al sistema operativo. Por ejemplo, los investigadores de Sophos detectaron que los ciberdelincuentes que distribuían el ransomware BlackByte explotaban los controladores RTCore64.sys y RTCore32.sys, usados por la popular utilidad de overclocking para la tarjeta gráfica Micro-Star MSI AfterBurner 4.6.2.15658. Una vulnerabilidad en estos controladores (CVE-2019-16098) permite a un usuario autenticado leer y escribir en la memoria arbitraria, que en este caso fue usada para eludir y desactivar parte del software de seguridad.

Otros incidentes recientes en los que se ha utilizado la técnica BYOVD incluyen el uso indebido de un controlador antitrampas vulnerable para el juego Genshin Impact en julio, y la detección en mayo de una variante del ransomware AvosLocker que explotaba un controlador antirootkit vulnerable de Avast. En ambos casos, los controladores fueron explotados para eludir o desactivar el software de seguridad.

En total, nuestro equipo de Rapid Response ha observado suficiente actividad como para determinar varias señales de aviso útiles que indican que un ataque de ransomware puede estar en camino. En una encuesta de los incidentes gestionados durante los primeros nueve meses de 2022, por lo menos un 83 % del ransomware fue precedido de algún tipo de señal de peligro. Los cinco precursores más comunes de un ataque de ransomware, junto con su respectiva clasificación MITRE ATT&CK, fueron:

- T1003 – Acceso a credenciales – Volcado de credenciales de SO
  - El volcado de credenciales, tanto en texto plano como con hash, para obtener información de inicio de sesión y credenciales del sistema operativo y el software atacados.
- T1562 – Evasión de defensa – Debilitación de las defensas
  - La modificación o la desactivación de componentes del entorno de la víctima para eludir o ralentizar las medidas de defensa activas, incluyendo tanto medidas de prevención como funciones de auditoría/registro.
- T1055 – Aumento de privilegios – Inyección de procesos
  - Inyección de código en el espacio de direcciones de procesos de confianza, lo que permite al código atacante evadir las defensas y/o aumentar los privilegios. La precarga y la carga lateral de DLL se incluyen en esta categoría.
- T1021 – Propagación lateral – Servicios remotos
  - Uso de servicios remotos vía cuentas válidas/sin protección para iniciar sesión en un sistema y realizar acciones como el usuario que ha iniciado sesión, posiblemente usando un RAT o un RAT de doble uso, según se ha descrito anteriormente.
- T1059 – Ejecución– Intérprete de comandos y scripting
  - Uso indebido de intérpretes de comandos y scripts para ejecutar comandos, scripts o binarios, o también mediante terminales interactivos o shells, o a través de servicios remotos, como se ha mencionado anteriormente.

Otros pocos patrones detectados de interés para los profesionales, aunque no tan claramente clasificados, fueron:

- El 64 % de los ataques de ransomware (específicamente, el despliegue del ransomware) se inició entre las 10 de la noche y las 6 de la mañana (hora local).
- El periodo de tiempo más común para el inicio de los ataques fue el «turno de noche» del lunes al martes.
- La exfiltración precedió a la fase de demanda del ransomware en aproximadamente dos días.
- La mediana del periodo de permanencia de los atacantes fue de 11 días.

Ransomware dirigido contras las actualizaciones de seguridad de endpoints

En la lista anterior de los precursores de un ataque de ransomware, el punto «T1562 – Evasión de defensa – Debilitación de las defensas» merece la pena ser desarrollado algo más. Uno de los hechos que más predominó en las intervenciones del equipo Rapid Response en 2022 refleja el éxito de Sophos a la hora de impedir que el ransomware cause daños y el reconocimiento de ese éxito por parte de los grupos dominantes de ransomware y sus afiliados: los ataques de ransomware ahora de forma rutinaria implican, como precursor de la implementación del malware de cifrado, intentos de acceso a los controles administrativos que gestionan la postura de seguridad del objetivo.

Como ya hemos descrito en una sección anterior, los «adversarios activos» del ransomware, las personas que intervienen con su teclado durante un ataque, utilizan habitualmente herramientas de rastreo de contraseñas o scraping para poder hacerse con las credenciales administrativas. Los atacantes explotan utilidades como Mimikatz, originalmente creada como una herramienta para mejorar la seguridad, para rastrear y extraer contraseñas de usuario de las redes de los objetivos del ataque.

Previamente, estas contraseñas administrativas se usaban para tomar el control de las herramientas de administración (como los controladores de dominio de Windows), que luego podían explotarse para desplegar el propio ransomware. Pero en los ataques más recientes, los atacantes están utilizando cada vez más estas credenciales para acceder a los controles centrales utilizados para administrar la protección de seguridad de los endpoints. En algunos casos, los atacantes usaron inmediatamente estas credenciales robadas para iniciar sesión en esas herramientas de administración centrales y desactivar las funciones de protección contra manipulaciones en esas herramientas de protección de endpoints o, en algunos casos, para desactivar por completo la seguridad de endpoints.

Para frustrar estos tipos de ataques, Sophos y otras empresas han añadido funciones de autenticación multifactor (MFA) en las páginas de inicio de sesión de la consola de administración central, así como en dispositivos físicos como firewalls, que tienen inicios de sesión administrativos. No obstante, los usuarios finales de estos productos (es decir, los administradores de seguridad y de TI) aún tienen que activar estas funciones y registrarse para usarlas antes de que puedan detener de forma efectiva a los atacantes. Sophos recomienda encarecidamente a todos sus clientes activar estas protecciones lo antes posible.

Malware minero

El software de criptominería consume potencia computacional para realizar tareas criptográficas con la esperanza de ganar nuevas «monedas» (tokens), normalmente participando en un pool de procesadores o equipos conectados en red. Para muchas criptomonedas, la minería requiere hardware especializado con unidades de procesamiento gráfico dedicadas específicamente a tareas que requieren elevadas capacidades de procesamiento. Pero sigue habiendo oportunidades para la explotación de hardware menos especializado para la criptominería, y hay extensas redes de bots mineros que se autopropagan que todavía siguen intentando explotar sistemas vulnerables y robar potencia de procesamiento para su beneficio.

Si bien este malware no tiene impacto sobre los datos de una organización, sí merma los recursos informáticos y eleva los costes eléctricos y de refrigeración. Y frecuentemente, el malware de criptominería es el precursor de otro malware, ya que normalmente se despliega a través de vulnerabilidades de red y software fácilmente explotables.

La mayoría del malware de extracción de criptodivisas se centra en Monero (XMR), por un número de razones. El tipo de trabajo necesario para producir XMR no requiere necesariamente tarjetas gráficas especializadas, lo que significa que se puede extraer con servidores con hardware gráfico básico. Y XMR es menos rastreable que muchas de las otras criptomonedas, lo que la convierte en más atractiva para la actividad delictiva.

Los bots mineros son frecuentemente el primer malware en explotar las vulnerabilidades recién publicadas. La vulnerabilidad Log4J Java y los exploits de ProxyLogon/ProxyShell de Microsoft Exchange Server fueron rápidamente explotados por redes de bots mineros. En muchos casos de ransomware observados por Rapid Response, Sophos encontró evidencias de que el malware minero estaba usando el mismo punto de entrada inicial que el ransomware, en algunos casos meses antes del ataque de ransomware.

Los mineros también son un problema multiplataforma. Si bien muchos de los bots de malware minero que Sophos detecta están basados en Windows (y aprovechan PowerShell y otros motores de scripting de Windows para su instalación y persistencia), también hay versiones de Linux de estas redes de bots, que frecuentemente se dirigen contra dispositivos de red o servidores web sin parchear.

Aunque los mineros XMR siguen siendo habituales y populares, las fluctuaciones (principalmente en dirección negativa) en el valor de algunas criptomonedas han tenido un efecto en los operadores de minería. Como el valor de XMR ha bajado, la rentabilidad de las redes de bots mineros ha caído, y parece que esto ha tenido un impacto en el esfuerzo que los operadores dedican a ampliar sus pools de minería. Algunas fluctuaciones en las tasas de detección de los despliegues de mineros han seguido las fluctuaciones del valor de XMR, según se muestra a continuación. Obsérvese de forma particular la caída a mediados de junio tanto del valor de XMR como de las detecciones de mineros.

Detecciones del minero Monero y fluctuaciones de precios, abril-septiembre de 2022

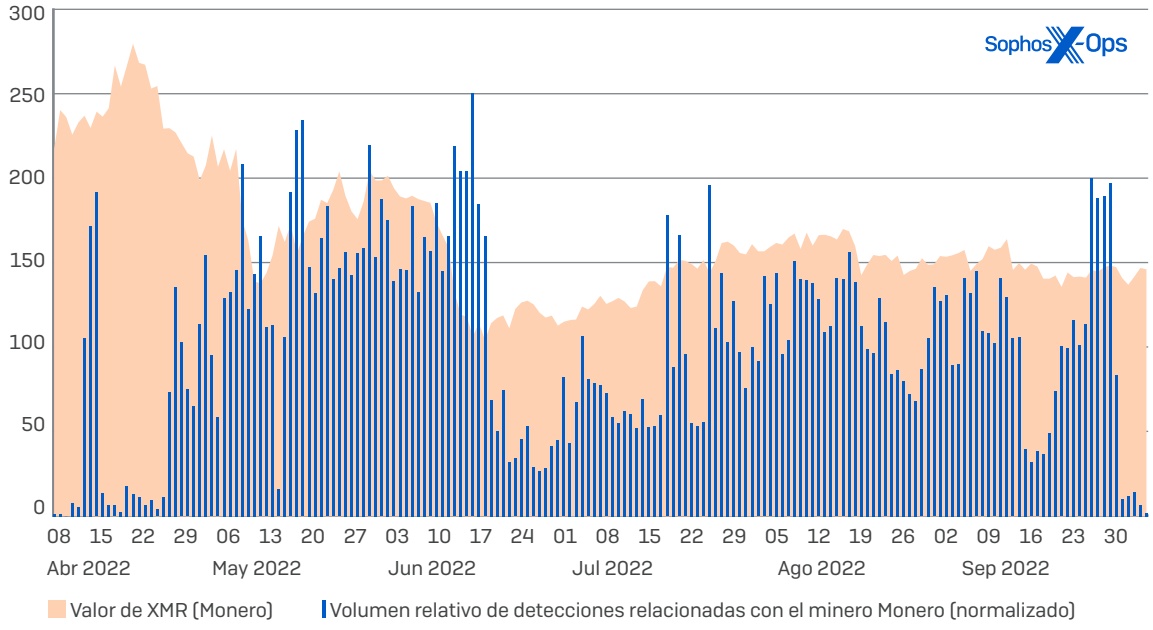

Fig. 35. Las detecciones de Monero durante el año pasado (en azul, totales normalizados en base a la escala) muestran algo de congruencia con los valores de Monero durante el periodo (en naranja).

Pero la rentabilidad de los mineros no solo se ve afectada por el valor de la divisa que se está extrayendo, sino también por la longevidad del minero. Muchos mineros en realidad buscan y eliminan los mineros similares de los servidores que explotan. En algunos casos, los mineros incluso despliegan parches para solucionar las vulnerabilidades que aprovecharon para su instalación a fin de prevenir que otros mineros los desbanquen, lo que les garantiza la persistencia cuando las organizaciones realizan escaneados en búsqueda de sistemas vulnerables.

Más allá de Windows: panorama de amenazas para Linux, Mac y dispositivos móviles

Hasta este momento en nuestro informe hemos estado hablando principalmente del malware y las herramientas de ataque que afectan a Windows. Algo que no nos debe extrañar, considerando el lugar preponderante que Windows ocupa en la lista de objetivos de la mayoría de los atacantes. Sin embargo, Windows no es el único objetivo viable en una organización, y cada vez más tenemos noticias de campañas con cargas «compatibles» con múltiples plataformas. Estas se crean usando lenguajes multiplataforma como Go o Python (frecuentemente compiladas en PyInstaller) o marcos como Electron, o preparando binarios para los marcos más importantes. En esta sección final echaremos un breve vistazo a los panoramas de amenazas para Linux, Mac y plataformas móviles, teniendo en cuenta que muchos de los mineros en particular están, de nuevo, presentes en estas y otras plataformas.

Amenazas para Linux

Los sistemas Linux llevan siendo desde hace mucho un objetivo para los servicios que con más frecuencia se implementan en ese sistema operativo, incluidos los sitios web de las organizaciones, los servidores de equipos virtuales, los dispositivos de red, los servidores de almacenamiento y la infraestructura de aplicaciones empresariales. Cada vez más, los delincuentes están desarrollando ransomware y otro malware multiplataforma que les permite dirigirse mejor contra esos recursos con fines lucrativos. En los primeros seis meses desde que Sophos presentó sus soluciones para Linux, hemos detectado 14 servidores Linux individuales que han sido objetivo del ransomware.

Gran parte del malware que afecta a los sistemas Linux (así como a otras plataformas de servidor) se crea para la extracción de criptomonedas. Más del 40 % de nuestras detecciones, y el 72 % de los dispositivos Linux individuales en los que se ha detectado malware, están relacionados con mineros.

Amenazas para Linux por porcentaje de detecciones en Linux		
Amenaza	**Porcentaje de detecciones**	**Notas**
Minero	43,0 %	Detección de minero genérico
DDoS	27,1 %	Detección relacionada con Mirai
Tsunami	12,3 %	Cliente DDoS basado en IRC
Gognt	11,5 %	Detección genérica para malware escrito en Go
Rst	1,3 %	Infector de archivos de 20 años
Loit	1,1 %	Exploit local
Swrort	0,9 %	Mettle (implementación de Meterpreter) para Linux
SSHDoor	0,7 %	Puerta trasera SSH
XpMmap	0,6 %	Exploits relacionados con la memoria
DrtyCoW	0,6 %	Exploit Dirty COW (CVE-2016-5195)
ProcHid	0,4 %	Troyano que oculta procesos
Ngioweb	0,2 %	Red de bots proxy
Psdon	0,1 %	Agente Poseidon para el marco de equipo rojo Mythic
GoScan	0,1 %	Escáner Go de búsqueda de equipos vulnerables

Fig. 36. A pesar del caos en el panorama de las criptomonedas en 2022, los mineros son, desafortunadamente, un tipo de infección fiable en Linux.

Sophos X-Ops

Los mineros han dominado los resultados de Linux este año, incluso más de lo que sugiere esta tabla. El término «minero» se refiere a la detección genérica de un criptominero por parte de Sophos. Los mineros también pueden detectarse con otros nombres; por ejemplo, «Gognt» es nuestra detección para familias de malware escritas en Go que, por lo demás, no están relacionadas. Esto significa que probablemente haya mineros que se queden fuera de la detección de «mineros», es decir, que incluso haya más de los que se muestran aquí.

Amenazas para Linux por porcentaje de detecciones únicas de Linux		
Amenaza	**Porcentaje de equipos únicos**	**Notas**
Minero	74,3 %	Detección de minero genérico
Gognt	5,1 %	Detección genérica para familias de malware escritas en Go
DDoS	4,3 %	Detección relacionada con Mirai
Swrort	3,2 %	Mettle (implementación de Meterpreter) para Linux
DrtyCoW	3,1 %	Exploit Dirty COW (CVE-2016-5195)
Ngioweb	2,8 %	Red de bots proxy
Tsunami	2,7 %	Cliente DDoS basado en IRC
Roopre	0,9 %	Puerta trasera dirigida contra servidores web
SSHBrut	0,9 %	Descifrador de contraseñas por fuerza bruta SSH
Loit	0,8 %	Exploit local
Shell	0,8 %	Malware que proporciona al atacante acceso a la shell
Bckdr	0,6 %	Detección de puerta trasera genérica
Ransm	0,6 %	Ransomware

Fig. 37. Cuando el desglose se realiza por máquinas únicas afectadas, el impacto de los mineros en Linux es todavía más claro.

Los siguientes grupos más grandes de detecciones en sistemas Linux afectados están asociados con Gognt y con kits de herramientas de denegación de servicio (DDoS). Prácticamente todas estas vulnerabilidades objetivo del malware han sido resueltas en las versiones más recientes de Linux, pero permanecen sin parchear en un número considerable de equipos y dispositivos.

Entre las principales amenazas restantes para Linux se encuentran varias puertas traseras y redes de bots, pero quizás la más interesante desde el punto de vista de las organizaciones sea Tsunami, una puerta trasera para Linux que existe desde hace bastante tiempo y que recientemente ha evolucionado para dirigirse contra servidores de aplicaciones Jenkins y Weblogic.

Amenazas para Mac

En 2022 observamos un número creciente de herramientas de ataque de código abierto y marcos posexploits/C2 compatibles con macOS disponibles en sitios como GitHub. La mera presencia de código en el repositorio no se correlaciona exactamente con una explosión inesperada de grandes ataques contra Mac, pero es probable que sí indique por lo menos un aumento del interés y de la voluntad de compartir dicho código.

En la plataforma macOS, la principal amenaza continúan siendo las aplicaciones no deseadas, incluidas las aplicaciones que instalan complementos para el navegador Safari de Apple (así como otras plataformas de navegador). Estas aplicaciones inyectan contenido en las páginas web con el fin de redireccionar a los usuarios a contenido fraudulento o malicioso.

Aplicaciones no deseadas (PUA) en macOS, abril-septiembre de 2022		
malware	**Porcentaje de equipos únicos**	**Notas**
Adloadr	16,2 %	Detección genérica de adware
Genieo	8,9 %	Secuestro del navegador (búsqueda)
Bundlore	8,4 %	Adware
Dynji	4,6 %	Secuestro del navegador (barra de herramientas)
Pirrit	3,7 %	Adware
AdvMac	3,2 %	Adware
HistColl	3,0 %	Recopilación de datos del navegador
Keygen	2,3 %	Herramienta de piratería de software

Fig. 38. Adloadr lidera la lista de PUA de Mac en 2022 con un margen amplio.

La aplicación Adloadr (una de las varias PUA predominantes, caracterizable como adware) se colocó en el primer puesto en nuestras estadísticas de telemetría de 2022 para Mac, con casi el doble de infecciones de equipos únicos que el secuestrador de navegadores Genieo, en segundo puesto.

En lo que respecta al malware, hemos observado cifras altas para NukeSped, VSearch y Dwnldr: un troyano de acceso remoto, un paquete de adware y un troyano descargador de aplicación general, respectivamente. Chropex y ProxAgnt, dos aplicaciones de ayuda asociadas con la familia Adloadr, también aparecieron en nuestra lista de detecciones comunes.

Detecciones de malware en macOS, abril-septiembre 2022		
malware	**Porcentaje de equipos únicos**	**Notas**
NukeSped	22,2 %	Troyano de acceso remoto
VSearch	15,6 %	Adware/secuestrador del navegador
Dwnldr	10,8 %	Detección de troyano genérico
Agent	10,8 %	Detección de malware genérico
Keygen	6,4 %	Generador de claves para eludir la protección anticopia
FkCodec	6,2 %	Adware; pretende ser un instalador de códecs de vídeo
Chropex	5,0 %	Adware; también presenta comportamiento de secuestrador del navegador
ProxAgnt	1,9 %	Troyano
Swrort	1,5 %	Troyano de acceso remoto

Fig. 39. NukeSped, VSearch y Dwnldr ocupan los primeros puestos en la clasificación de detecciones de malware para macOS.

Hasta octubre, hemos detectado cinco nuevas amenazas para macOS que han surgido en 2022. Ninguna ha logrado situarse entre las principales de nuestras listas de malware para macOS, pero observamos con interés cada nueva detección.

Nuevas amenazas para macOS observadas en 2022			
Mes	**Nombre**	**malware**	**Notas**
Enero	SysJoker	OSX/SysJoker	Puerta trasera multiplataforma compatible con macOS
Enero	DazzleSpy	OSX/DazzleSpy	Técnica de infección relacionada con MACMA, una puerta trasera que actuó contra activistas en favor de la democracia en Hong Kong
Marzo	Gimmick	OSX/Gimmick	Se comunica con las API de Google Drive para ocultar el tráfico de red de los sistemas de monitorización
Mayo	pymafka/CrateDepression	Troj/Pymaf, OSX/Cobalt	Ataque a la cadena de suministro en paquete alojado en PyPI; finalmente inyecta una carga Beacon de Cobalt Strike
Octubre	Alchimist	Exp/20214034-D	Marco de ataque multiplataforma escrito en Go

Fig. 40. En los primeros diez meses de 2022 debutaron cinco amenazas nuevas para macOS.

Amenazas para dispositivos móviles

Dado que las aplicaciones móviles se han convertido en la forma dominante de interactuar con Internet, los dispositivos móviles se encuentran en el centro de una gama cada vez mayor de nuevos tipos de ciberdelincuencia. Aunque la plataforma Android sigue experimentando un flujo continuo de malware en forma de aplicaciones falsas y ladrones de información, tanto Android como iOS se han convertido cada vez en el objetivo de aplicaciones fraudulentas y falsas, y los ciberdelincuentes han encontrado formas de usar la ingeniería social para irrumpir incluso en el jardín amurallado de los dispositivos móviles de Apple.

Los inyectores de malware, el spyware y el malware asociado a la banca siguen estando a la cabeza en lo que se refiere a paquetes .APK maliciosos para Android en nuestras detecciones, junto con las aplicaciones que generan clics falsos en anuncios. Pero las aplicaciones no deseadas (incluidas las que básicamente no hacen otra cosa que recaudar «compras desde las propias apps» ocultas de las víctimas) continúan creciendo como una amenaza para los usuarios de dispositivos móviles. Y en el último año hemos visto la aparición de un sofisticado conjunto de redes de fraude financiero, que utiliza aplicaciones falsas y se ha convertido en una industria en el sudeste asiático.

Sophos comenzó en 2021 a hacer el seguimiento de una campaña de crimen organizado que hemos llamado CryptoRom. La campaña está basada en un forma de ciberfraude, conocida como sha zhu pan (杀猪盘), que literalmente significa «tabla de matanza de cerdos» en chino. Está respaldada por un sindicato bien organizado de desarrolladores de páginas web y aplicaciones fraudulentas, creadores de perfiles sociales falsos y personas que usan guiones de ingeniería social en las redes sociales y las aplicaciones de citas para estafar a las víctimas.

En octubre de 2021 documentamos la expansión global de la campaña. La fórmula ha cambiado, pasando de inversiones en criptomonedas falsas a inversiones en criptoderivados falsos, expandiéndose a otros mercados financieros falsos. Para que estas maquinaciones parezcan legítimas, las redes de fraude crean aplicaciones y sitios web falsos para dispositivos móviles que se hacen pasar por instituciones financieras legítimas. Muchas de estas apps se han colado sin ser detectadas en las tiendas de apps, como las aplicaciones de «minería de liquidez» que se encontraron en Apple App Store y Google Play Store.

Mientras tanto, los estafadores han encontrado formas para explotar también iOS, aprovechando clips web y programas de implementación de prueba de desarrolladores de aplicaciones para hacer llegar sus aplicaciones a dispositivos iOS. Esto incluye explotar el esquema de distribución ad hoc «Super Signature», las pruebas beta «Test Flight» y los esquemas de aplicaciones para empresas de Apple para evitar los controles de seguridad del App Store de Apple. El mismo enfoque puede ser usado para otro malware dirigido contra iOs, pero requiere cierta ingeniería social en el objetivo para que la instalación pueda prosperar.

Estas aplicaciones han provocado cientos de millones de dólares en pérdidas a las víctimas, y son parte de un creciente ecosistema de ciberdelincuencia que va desde estafas románticas hasta intentos más amplios de ingeniería social en plataformas como Facebook, Twitter y LinkedIn. Estos fraudes siguen evolucionando y son copiados por otras bandas delictivas, con su propia impronta particular.

Tanto Android como iOS también son objetivos de campañas publicitarias maliciosas, incluyendo alertas falsas que imitan las alertas del sistema, y que a menudo dirigen a los usuarios a una tienda de apps para comprar una aplicación que tiene cuotas de suscripción ocultas, que instala otro malware o que hace ambas cosas.

Sophos continúa trabajando en métodos para bloquear estas amenazas y alerta a los desarrolladores de SO móviles sobre nuevos exploits en sus tiendas de aplicaciones a medida que son descubiertos.

Conclusión

En todo el panorama de las amenazas, destacan dos cosas: un terreno de juego cada vez más accesible para los ciberdelincuentes incipientes y la comercialización de lo que hasta ahora se habían considerado herramientas y tácticas de «amenazas avanzadas recurrentes». Aunque desde hace mucho tiempo existe un próspero mercado de herramientas de hacking, malware y acceso a redes vulnerables, las lecciones aprendidas de la reciente historia de las operaciones de ransomware y otros atacantes maliciosos bien financiados están cada vez más al alcance de la comunidad criminal en general, al igual que las herramientas de seguridad disponibles en el mercado diseñadas para burlar ciertas defensas.

Las condiciones geopolíticas han seguido dificultando la lucha contra la ciberdelincuencia. Este año, China ha dado por terminada la cooperación con EE. UU. en materia legislativa de lucha contra la ciberdelincuencia debido al aumento de tensiones entre ambos países. Mientras tanto, a medida que China ha aumentado su persecución de los fraudes de criptomonedas y otros ciberdelitos en el país, los delincuentes de idioma chino han cambiado rápidamente de estrategia y pasado a exportar estas operaciones delictivas. Y aunque la guerra en Ucrania interrumpió brevemente la actividad de algunas bandas de delincuentes de idioma ruso, estas se reconstituyeron rápidamente.

No hay una defensa segura contra todas estas amenazas. La defensa activa es necesaria para prevenir que las incursiones ocasionen daños, y la carga de la defensa es demasiado grande como para que muchas organizaciones puedan afrontarla por sí mismas. Sophos continúa trabajando para aumentar su capacidad de ayuda a organizaciones de todo tamaño contra el panorama de amenazas en constante evolución mediante soluciones de defensa para endpoints y redes y servicios de operaciones de seguridad gestionadas.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

17-11-22 ES (NP)

SOPHOS