CARGADORES DE RANSOMWARE Y PRODUCTOS BÁSICOS

DESCARGA EL INFORME COMPLETO EN INGLÉS AQUÍ

PANORAMA DE AMENAZAS DE RANSOMWARE

El espacio de ransomware es dinámico y se adapta continuamente a los cambios en el entorno geopolítico, las acciones de los defensores y los esfuerzos que hacen las fuerzas del orden público, que aumentaron en alcance e intensidad en 2022. Esto lleva a los grupos a cambiar la marca con diferentes nombres, cerrar operaciones y formar nuevas asociaciones estratégicas. Cisco Talos observó varias tendencias relacionadas a lo largo de 2022.

Talos sigue a más de una docena de grupos de ransomware como servicio (RaaS) **(Figura 1)**. Según nuestros hallazgos, LockBit fue el grupo más activo en 2022, lo que representó más del 20 por ciento de la cantidad total de publicaciones de víctimas de la web oscura, seguido de cerca por Hive y Black Basta. Estos hallazgos apuntan a una mayor democratización de los adversarios del ransomware, un cambio general respecto de años anteriores en los que unos pocos grupos selectos monopolizaron el panorama. Los afiliados de ransomware ya no están estructurados en silos y ahora trabajan en varios grupos, donde los actores con conjuntos de habilidades únicas tienen más oportunidades para respaldar varias campañas y organizaciones.

También hubo una mayor fricción en toda la comunidad, ya que la guerra en Ucrania obligó a muchos agentes de amenazas a elegir lados en el conflicto y dirigir sus operaciones contra objetivos a favor de los rusos o los ucranianos. El grupo de RaaS Conti fue uno de los más ruidosos y advirtió que atacaría a cualquiera que intentara interferir con la invasión por parte de Rusia. Un individuo relacionado con Conti se vengó de la banda de ransomware filtrando información, incluido el código fuente del malware y los chats internos entre los afiliados. En otro evento, Talos se dio cuenta de la divulgación de un constructor filtrado para el cifrador de ransomware LockBit 3.0, denominado “LockBitBlack”. El individuo que se responsabiliza es un supuesto desarrollador de LockBit que, según LockBit, afirmó que estaba descontento con la estructura de pago del grupo.

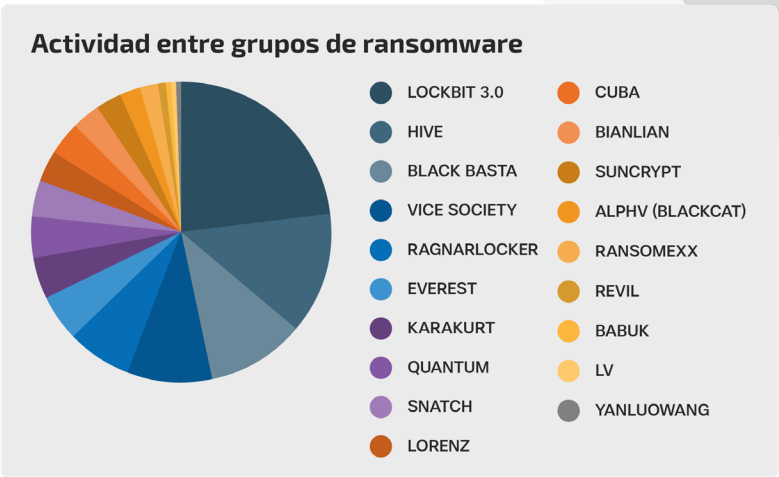

Figura 1. *Cantidad de publicaciones realizadas en sitios de filtración de datos de ransomware rastreados por Talos, de enero a octubre.*

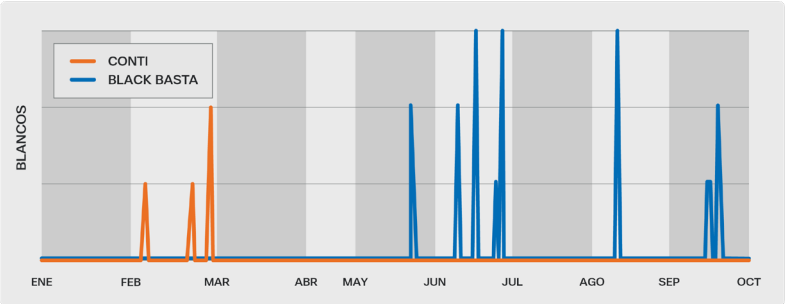

Figura 2. *Detecciones de indicadores de comportamiento en Secure Malware Analytics para el ransomware Conti y modificaciones del registro Black Basta.*

Este tipo de fricción es lo que a menudo conduce al cambio de marca de las bandas de ransomware o al surgimiento de nuevos grupos. Cuando Conti cesó las operaciones y desconectó su infraestructura, vimos una caída general en las detecciones en nuestra telemetría, pero poco después, surgió un cambio de marca de Conti denominado “Black Basta”. Los investigadores sugieren que los dos grupos tienen sitios web y estilos de comunicación de pago y filtración similares **(Figura 2)**.

CARGADORES DE PRODUCTOS BÁSICOS

Los cargadores de productos básicos (troyanos comerciales que implementan malware de segunda etapa) son una amenaza constante que continúa teniendo un impacto global. Desarrollados inicialmente como troyanos bancarios pensados para comprometer a las entidades a fin de obtener ganancias monetarias, con el tiempo se han adaptado

© 2023 Cisco y/o sus filiales. Todos los derechos reservados. | talosintelligence.com

CARGADORES DE RANSOMWARE Y PRODUCTOS BÁSICOS

a mayores controles de seguridad y se han convertido en amenazas mucho más sofisticadas. Ahora operan principalmente como cargadores con funciones modulares, lo que permite a los ciberdelincuentes la flexibilidad de trabajar con una variedad de herramientas de código abierto y malware recientemente desarrollado. Los cuatro cargadores de productos básicos más activos en 2022 fueron Qakbot, Emotet, IcedID y Trickbot, según nuestro análisis de varios conjuntos de telemetría de red y terminales **(Figura 3)**.

Aunque nuestra telemetría detectó actividad asociada con Trickbot, evaluamos que gran parte de esta actividad probablemente detectaba terminales antiguos e infectados, ya que los operadores de malware han estado inactivos desde principios de 2022. De manera similar, Emotet, aunque sigue operativo, sigue siendo significativamente menos activo que antes de que las autoridades desmantelaran el botnet a principios de enero de 2021. Otro malware ha llenado el vacío al volverse más popular, como Qakbot e IcedID.

En una tendencia general en 2022 que observamos, los operadores entregaron con mayor frecuencia Qakbot, Emotet e IcedID mediante tipos de archivos ISO, ZIP y LNK, lo que probablemente eludiría los esfuerzos de Microsoft para bloquear documentos habilitados para macros. En otra tendencia, Talos observó que los operadores de Qakbot, Emotet e IcedID descargaban y lanzaban cargas útiles maliciosas mediante binarios externos (LoLBins) que se encuentran en los entornos de las víctimas. En algunos casos, las filiales de Qakbot y Emotet refinaron su secuencia de ataque y experimentaron con diferentes LoLBins para mejorar sus posibilidades de pasar desapercibidas dentro de una organización.

Aunque nuestra telemetría detectó actividad asociada con Trickbot, evaluamos que gran parte de esta actividad probablemente detectaba terminales antiguos e infectados, ya que los operadores de malware han estado inactivos desde principios de 2022. De manera similar, Emotet, aunque sigue operativo, sigue siendo significativamente menos activo que antes de que las autoridades desmantelaran el botnet a principios de enero de 2021. Otro malware ha llenado el vacío al volverse más popular, como Qakbot e IcedID.

Una revisión en profundidad de cada cargador de productos está disponible en el informe completo.

Cargadores de productos básicos

	Qakbot	IcedID	Emotet	Trickbot
Alias	Quackbot, Qbot, Pinkslipbot	BokBot	Geodo	No corresponde
Afiliaciones	Malware para productos básicos probablemente desarrollado por ciberdelincuentes eurasiáticos	Desconocido	Malware para productos básicos desarrollado por Mummy Spider, un grupo de delitos cibernéticos alineado con Rusia	Malware para productos básicos desarrollado por Wizard Spider, un grupo de delitos cibernéticos alineado con Rusia
Activo desde	2007	2014	2017	2016

Objetivos

- Obtener acceso inicial y establecer la persistencia para facilitar más actividades de intrusión.
- Implementar malware de próxima etapa, incluido el ransomware.

Victimología

- Se dirige a todos los sectores de todo el mundo.
- Desde la guerra entre Rusia y Ucrania, Trickbot ha amenazado con tomar represalias contra los ataques percibidos contra el pueblo ruso.

TTP destacados

- Suplantación de identidad (phishing), correo electrónico no deseado, ingeniería social, explotación de vulnerabilidades, robo de datos, como datos y credenciales financieras, y propagación similar a la de los gusanos.
- Altamente modular, lo que permite a los operadores realizar una amplia gama de ataques.

Malware y herramientas

- Las variantes de malware implementan y son implementadas por varias otras familias de malware, incluidas entre sí.
- Utilice herramientas comerciales tales como Cobalt Strike y LoLbins en diversas etapas del ciclo de vida del ataque.

Figura 3. *Matriz de amenazas de cargadores de productos básicos.*

© 2023 Cisco y/o sus filiales. Todos los derechos reservados. | talosintelligence.com