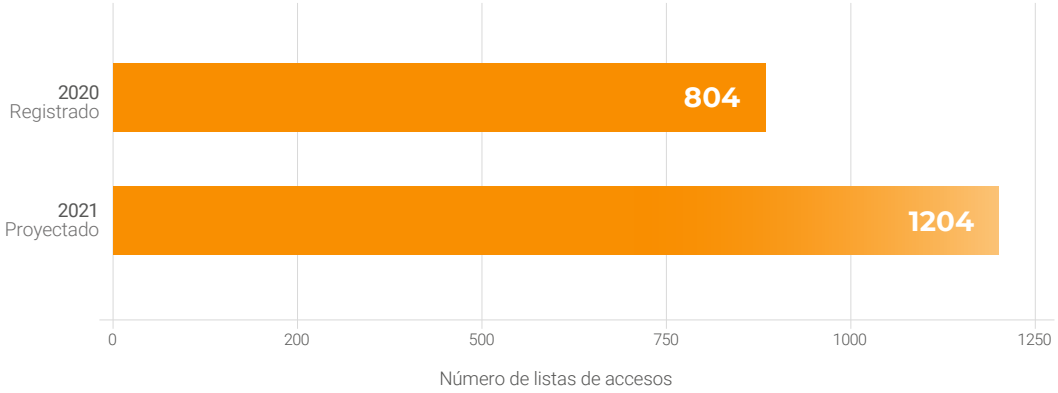
Flashcard Report:
La Monetización del Cibercrimen

Se ha incrementado la actividad del mercado de credenciales de acceso a redes

Tal como se puede ver en el siguiente gráfico, se ha identificado un aumento acelerado en la actividad de los mercados de la dark web que comercian con credenciales de acceso a redes comprometidas. Este negocio ha evolucionado hasta el punto de comerciar elementos que eran poco frecuentes hace unos años, ya que solían centrarse principalmente en la venta de datos de tarjetas de crédito comprometidas.



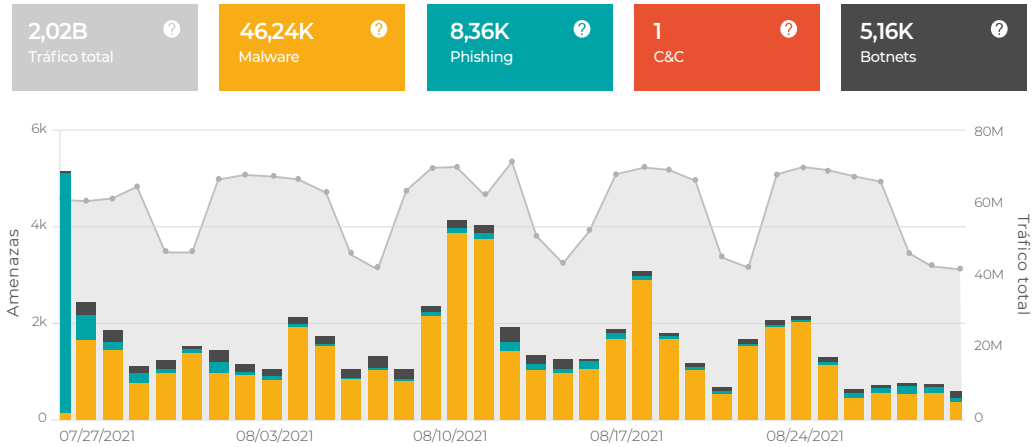
Venta de listas de accesos
2020 - 2021

Fuente:
"All Access Pass: Five Trends with Initial Access Brokers", ke-la.com (datos totales de 2020 y 2021 correspondientes a extrapolación de datos de H2 2020 y H1 2020 respectivamente)

Aunque obtener datos de tarjetas de crédito de forma fraudulenta facilitaba la monetización del cibercrimen, hemos sido testigos de un incremento en la monetización de cualquier actividad asociada al cibercrimen, especialmente de aquellos elementos que no son igual de rentables que los datos de tarjetas de crédito.

Una explicación del crecimiento de demanda

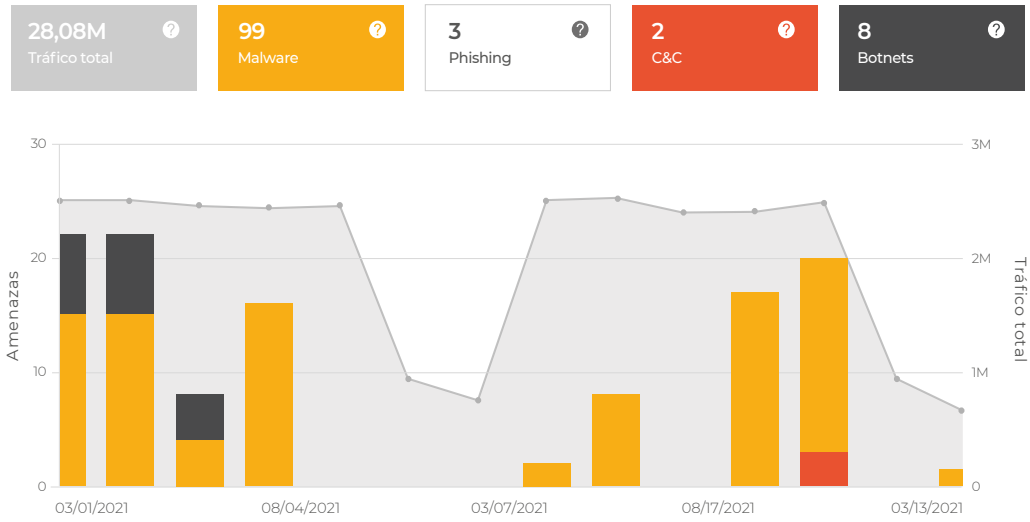
Haciendo un análisis de correlación de trazas de contacto en redes que han sido comprometidas con ransomware, se puede explicar el origen de la demanda que impulsa la aceleración observada en los mercados de la dark web.



En esta imagen correspondiente al portal de Lumu, se observa cómo un ataque de phishing condujo a la instalación de un botnet de criptojacking (gris oscuro), malware (amarillo) y, finalmente, un contacto solitario de C&C (rojo, no visible a esta escala).

La imagen muestra que mucho antes de que se materialice un incidente de ransomware, las redes de las organizaciones comprometidas evidencian un exagerado número de actividades que rara vez se asocian con incidentes de ransomware, como el phishing, los contactos frecuentes con botnets de minería de criptomonedas y la interacción con botnets de spam.

Los incidentes modernos de ransomware requieren tiempo para comprometer tantos activos como sea posible, interrumpir las operaciones de forma drástica, extraer la mayor cantidad de datos y ejercer la máxima presión a través de la extorsión. Este tiempo varía en función del propósito, los recursos, la forma de operar y las habilidades de los cibercriminales.

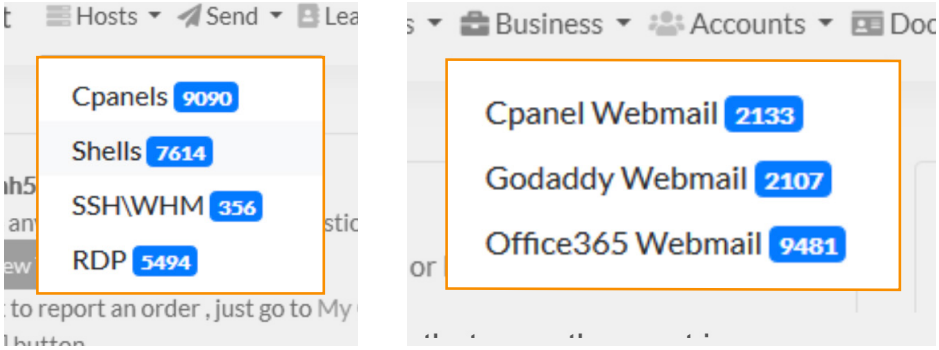


Esta imagen del Portal Lumu muestra cómo un ataque que inicialmente comenzó con criptojacking (gris oscuro) y malware (amarillo) derivó en un contacto de C&C (rojo) con la infraestructura del ransomware REvil/Sodinokibi.

Sin embargo, mientras el ataque de ransomware madura, los delincuentes buscan maximizar la monetización de la organización comprometida. Por ejemplo, es común ver la utilización de minado de criptomonedas el cual aprovecha los equipos de cómputo conectados a la red, o revende la infraestructura comprometida mediante el lanzamiento de campañas de spam para comprometer dispositivos adicionales de la misma organización. De este modo, diversos tipos de credenciales de acceso a estas redes comprometidas acaban en los mercados de la dark web.

Donde hay voluntad, hay un camino

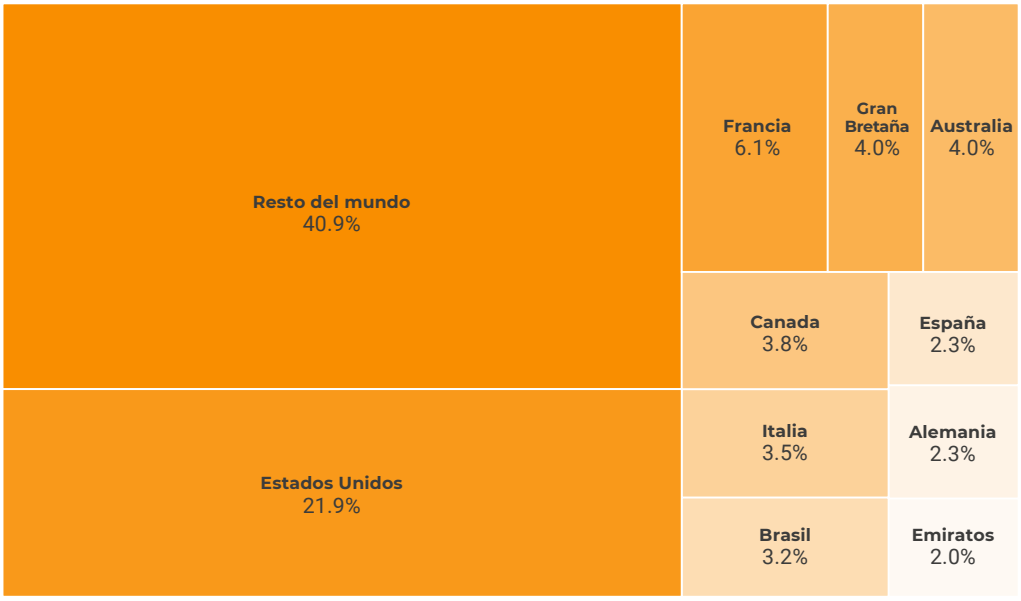
Como se puede ver anteriormente, un ataque de ransomware casi nunca es un hecho aislado. El ataque suele comenzar con un compromiso "menor", que se lanza fácilmente a través del acceso que ofrecen los mercados de credenciales online.



Captura de pantalla de un foro de la dark web en el que se vende el acceso a varios tipos de ingreso inicial a redes comprometidas.

Estos mercados ofrecen acceso a todo, desde paneles de administración de web hosting y servidores de correo electrónico, hasta acceso a escritorios remotos. Las organizaciones comprometidas abarcan todos los países, sectores y tamaños.

Las credenciales ofrecen un acceso fácil a la red



Top-10 de países donde se ubican las víctimas.
Más de 1.000 listas de acceso analizadas

Fuente: "All Access Pass: Five Trends with Initial Access Brokers", ke-la.com

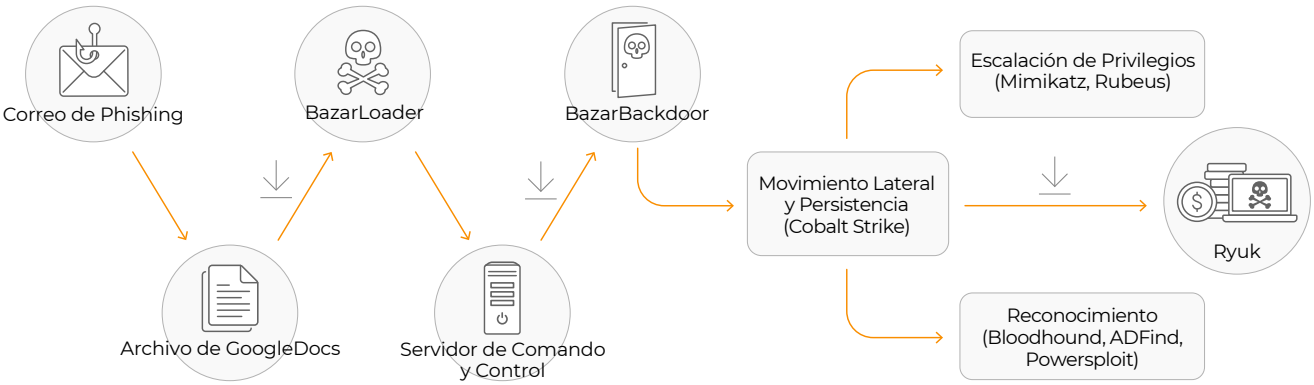
El acceso a los Protocolos de Escritorio Remoto (RDP) puede significar que el agente amenazante tiene el control de su red. El acceso a RDP permite que los ataques evadan la detección a través de VPN o SDP, como en el caso de la empresa de tratamiento de aguas de la Florida, donde los atacantes pudieron alterar la acidez del agua hasta niveles peligrosos. Este y otros tipos de acceso establecen la base perfecta para moverse lateralmente por toda la red.

Las técnicas de monetización varían

Hay muchas maneras de que los agentes amenazantes ganen dinero con su red. Estas incluyen:

- Botnets de minería de criptomonedas
- Botnets de spam
- Instalaciones de Adware
- Implantar/desplegar otro malware
- Vender puertas traseras de acceso a la red
- Extracción de información confidencial
- Extracción de datos de tarjetas de crédito
- Extorsión
- Ransomware

Los ataques evolucionan con diferentes técnicas



El “ransomware como servicio” (Ransomware as a Service en inglés) es un modelo de negocio bien establecido en el que se puede comprar ransomware a un precio muy bajo y que requiere habilidades mínimas para su manipulación y usufructo. A partir de abril de 2019, los agentes amenazantes empezaron a utilizar el malware tradicional para penetrar y establecerse en una empresa que pudieran vender a los especialistas en ransomware, en una táctica llamada malware- delivery-as-a-service. Esto ha llevado a la aparición de "cadenas de ransomware" en las que el ataque de ransomware está precedido por la utilización de un tipo de malware asociado.

Algunas cadenas de ransomware son:

- Emotet → TrickBot → Ryuk
- IcedID → REvil / Sodinokibi
- Qakbot → Egregor
- Zloader → DarkSide

No hay amenazas "menores"

La forma más fácil y rápida de monetizar el acceso a la red es a través de los botnets. Por lo tanto, este suele ser el primer tipo de compromiso que se ve en la red. Los cibercriminales siempre buscarán la vía de menor resistencia, menor esfuerzo y mayor impacto para perpetuar sus ataques. El ataque se intensificará cuando el atacante tenga suficientes recursos, tiempo y pruebas de que el ataque de ransomware va a representar una alta probabilidad de monetización y que la misma será de un alto valor. Los ataques de ransomware tardan tan solo tres días en madurar desde el compromiso inicial.

Recomendamos a las organizaciones que traten todos los compromisos como evidencia de un ataque serio en curso. Abra una cuenta de Lumu Free para conocer desde ya su exposición en tiempo real y su nivel de compromiso.