Microsoft Security

Ransomware como servicio: la nueva cara de la ciberdelincuencia industrializada

El modelo de negocio más reciente de los ciberdelitos, los ataques operados por humanos, alientan a delincuentes de habilidades particulares.

El ransomware, una de las ciberamenazas más persistentes y generalizadas, sigue evolucionando, y su forma más reciente presenta una nueva amenaza para las organizaciones de todo el mundo. La evolución del ransomware no implica nuevos avances en tecnología. En cambio, conlleva un nuevo modelo de negocio: ransomware como servicio (RaaS).

Ransomware como servicio (RaaS) es un acuerdo entre un operador que desarrolla y mantiene las herramientas para impulsar operaciones de extorsión y un afiliado que implementa la carga útil de ransomware. Cuando el afiliado lleva a cabo un ataque de ransomware y extorsión exitoso, ambos perfiles se benefician de ello.

El modelo de RaaS reduce los obstáculos de entrada para los atacantes, que pueden no tener las habilidades o los medios técnicos para desarrollar sus propias herramientas, pero pueden administrar pruebas de penetración listas para usar y herramientas de sysadmin para llevar a cabo ataques. Estos delincuentes de nivel inferior también pueden simplemente comprar acceso a la red de un grupo delictivo que ya ha vulnerado un perímetro.

Si bien los afiliados de RaaS utilizan cargas útiles de ransomware proporcionadas por operadores más sofisticados, no son parte de la misma "pandilla" de ransomware. Más bien, tienen sus propias empresas específicas que operan en la economía general de los ciberdelincuentes.

El avance de las capacidades de los ciberdelincuentes y el crecimiento de la economía global de la ciberdelincuencia

El modelo de ransomware como servicio ha facilitado un refinamiento rápido y la industrialización de lo que los delincuentes con menos capacidades pueden lograr. En el pasado, es posible que estos delincuentes menos sofisticados hubieran utilizado malware básico que desarrollaban o compraban para llevar a cabo ataques de alcance limitado, pero ahora pueden obtener todo lo que necesitan, desde acceso a redes hasta cargas útiles de ransomware, de sus operadores de RaaS (por un precio, por supuesto). Además, muchos programas de RaaS incorporan un conjunto de ofertas de soporte de extorsión, que incluye el hospedaje y la integración de sitios vulnerables en notas de rescate, así como una negociación de descifrado, presión de pago y servicios de transacciones de criptomonedas.

Esto significa que el impacto de un ataque exitoso de ransomware y extorsión sigue siendo el mismo, independientemente de las habilidades del atacante.

Detección y exploración de las vulnerabilidades de la red... por un precio

Una forma en que los operadores de RaaS aportan valor a sus afiliados es mediante el acceso a redes comprometidas. Los agentes de acceso examinan la Internet en busca de sistemas vulnerables que puedan comprometer y reservar para obtener ganancias en otro momento.

Para tener éxito, los atacantes necesitan credenciales. Las credenciales comprometidas son tan importantes para estos ataques, que cuando los ciberdelincuentes venden el acceso a la red, en muchos casos el precio incluye una cuenta de administrador garantizada.

Lo que hacen los delincuentes con su acceso una vez que lo han obtenido puede variar enormemente en función de los grupos y sus cargas de trabajo o motivaciones. Por lo tanto, el tiempo entre el acceso inicial a una implementación práctica de teclado puede ir de minutos a días o más, sin embargo, cuando las circunstancias lo permiten, el daño se puede infligir a una velocidad impresionante. De hecho, se ha observado que el tiempo desde el acceso inicial hasta el rescate completo (incluida la entrega de un agente de acceso a un afiliado de RaaS) es de menos de una hora.

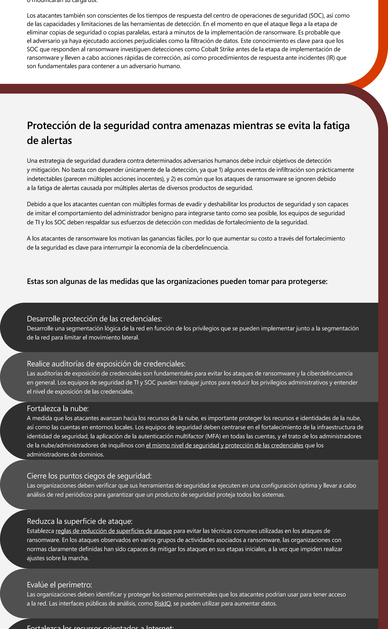
Métodos de acceso persistentes y sigilosos para mantener la economía en movimiento

Una vez que los atacantes obtienen acceso a una red, detestan marcharse, incluso después de haber cobrado su rescate. De hecho, es posible que el pago del rescate no reduzca el riesgo para una red afectada y que potencialmente solo sirva para financiar a los ciberdelincuentes, que seguirán intentando monetizar los ataques con diferentes cargas útiles de malware o ransomware hasta que sean expulsados.

El traspaso que se produce entre diferentes atacantes como transiciones en la economía de la ciberdelincuencia significa que múltiples grupos de actividad pueden permanecer en un entorno utilizando diversos métodos, distintos de las herramientas utilizadas en un ataque de ransomware. Por ejemplo, el acceso inicial que se obtiene mediante un troyano bancario conduce a una implementación de Cobalt Strike, pero el afiliado de RaaS que adquirió el acceso puede optar por usar una herramienta de acceso remoto como TeamViewer para operar su campaña.

El uso de herramientas y configuraciones legítimas para permanecer, en contraposición a implantes de malware como Cobalt Strike, es una técnica popular entre los atacantes de ransomware para evitar que se les detecte y así seguir residiendo en una red por más tiempo.

Otra técnica popular de los atacantes es crear nuevas cuentas de usuarios de puerta trasera, locales o en Active Directory, que se pueden agregar a herramientas de acceso remoto como una red privada virtual (VPN) o Escritorio remoto. También se ha observado que los atacantes de ransomware editan la configuración de los sistemas para habilitar Escritorio remoto, reducir la seguridad del protocolo y agregar nuevos usuarios al grupo de usuarios de Escritorio remoto.



Cómo enfrentar a los adversarios más escurridizos y astutos del mundo

Una de las cualidades de RaaS que hace que la amenaza sea tan preocupante es cómo se basa en atacantes humanos que pueden tomar decisiones informadas y calculadas, además de variar los patrones de ataque en función de lo que encuentran en las redes donde aterrizan, para asegurar así el cumplimiento de sus objetivos.

Microsoft acuñó el término ransomware operado por humanos para definir esta categoría de ataques como una cadena de actividad que culmina en una carga útil de ransomware, no como un conjunto de cargas útiles de malware que se bloquearán.

Si bien la mayoría de las campañas de acceso inicial se basan en el reconocimiento automatizado, una vez que el ataque pasa a la fase de ajustes sobre la marcha, los atacantes utilizarán su conocimiento y sus habilidades para intentar vencer a los productos de seguridad en el entorno.

A los atacantes de ransomware los motivan las ganancias fáciles, por lo que aumentar su costo a través del fortalecimiento de la seguridad es clave para interrumpir la economía de la ciberdelincuencia. Esta toma de decisiones humana significa que incluso si los productos de seguridad detectan etapas específicas de un ataque, los atacantes no se expulsan por completo, sino que intentan continuar si no se les bloquea mediante un control de seguridad. En muchos casos, si un producto antivirus detecta y bloquea una herramienta o carga útil, los atacantes simplemente se apropiarán de una herramienta diferente o modificarán su carga útil.

Los atacantes también son conscientes de los tiempos de respuesta del centro de operaciones de seguridad (SOC), así como de las capacidades y limitaciones de las herramientas de detección. En el momento en que el ataque llega a la etapa de eliminar copias de seguridad o copias parásitas, estará a minutos de la implementación de ransomware. Es probable que el adversario ya haya ejecutado acciones perjudiciales como la filtración de datos. Este conocimiento es clave para que los SOC que responden al ransomware investiguen detecciones como Cobalt Strike antes de la etapa de implementación de ransomware y lleven a cabo acciones rápidas de corrección, así como procedimientos de respuesta ante incidentes (IR) que son fundamentales para contener a un adversario humano.

Protección de la seguridad contra amenazas mientras se evita la fatiga de alertas

Una estrategia de seguridad duradera contra determinados adversarios humanos debe incluir objetivos de detección y mitigación. No basta con depender únicamente de la detección, ya que 1) algunos eventos de infiltración son prácticamente indetectables (parecen múltiples acciones inocentes), y 2) es común que los atacantes de ransomware se ignoren debido a la fatiga de alertas causada por múltiples alertas de diversos productos de seguridad.

Debido a que los atacantes cuentan con múltiples formas de evadir y deshabilitar los productos de seguridad y son capaces de imitar el comportamiento del administrador benigno para integrarse tanto como sea posible, los equipos de seguridad de TI y los SOC deben respaldar sus esfuerzos de detección con medidas de fortalecimiento de la seguridad.

A los atacantes de ransomware los motivan las ganancias fáciles, por lo que aumentar su costo a través del fortalecimiento de la seguridad es clave para interrumpir la economía de la ciberdelincuencia.

Estas son algunas de las medidas que las organizaciones pueden tomar para protegerse:

Desarrolle protección de las credenciales:
Desarrolle una segmentación lógica de la red en función de los privilegios que se pueden implementar junto a la segmentación de la red para limitar el movimiento lateral.

Realice auditorías de exposición de credenciales:
Las auditorías de exposición de credenciales son fundamentales para evitar los ataques de ransomware y la ciberdelincuencia en general. Los equipos de seguridad de TI y SOC pueden trabajar juntos para reducir los privilegios administrativos y entender el nivel de exposición de las credenciales.

Fortalezca la nube:
A medida que los atacantes avanzan hacia los recursos de la nube, es importante proteger los recursos e identidades de la nube, así como las cuentas en entornos locales. Los equipos de seguridad deben centrarse en el fortalecimiento de la infraestructura de identidad de seguridad, la aplicación de la autenticación multifactor (MFA) en todas las cuentas, y el trato de los administradores de la nube/administradores de inquilinos con el mismo nivel de seguridad y protección de las credenciales que los administradores de dominios.

Cierre los puntos ciegos de seguridad:
Las organizaciones deben verificar que sus herramientas de seguridad se ejecuten en una configuración óptima y llevar a cabo análisis de red periódicos para garantizar que un producto de seguridad proteja todos los sistemas.

Reduzca la superficie de ataque:
Establezca reglas de reducción de superficies de ataque para evitar las técnicas comunes utilizadas en los ataques de ransomware. En los ataques observados en varios grupos de actividades asociados a ransomware, las organizaciones con normas claramente definidas han sido capaces de mitigar los ataques en sus etapas iniciales, a la vez que impiden realizar ajustes sobre la marcha.

Evalúe el perímetro:
Las organizaciones deben identificar y proteger los sistemas perimetrales que los atacantes podrían usar para tener acceso a la red. Las interfaces públicas de análisis, como RiskIQ, se pueden utilizar para aumentar datos.

Fortalezca los recursos orientados a Internet:
Los atacantes de ransomware y los agentes de acceso utilizan las vulnerabilidades sin parches, independiente de si ya fueron reveladas o si son de día cero, en especial en la etapa de acceso inicial. También adoptan las nuevas vulnerabilidades con rapidez. Para reducir aún más la exposición, las organizaciones pueden usar las capacidades de administración de amenazas y vulnerabilidades en la detección de puntos de conexión y productos de respuesta para detectar, priorizar y corregir vulnerabilidades y configuraciones erróneas.

Prepárese para la recuperación:
La mejor defensa contra ransomware debe incluir planes para recuperarse rápidamente en caso de un ataque. Costará menos recuperarse de un ataque que pagar un rescate, así que asegúrese de realizar copias de seguridad periódicas de sus sistemas críticos y proteja esas copias de seguridad contra borrado y cifrado deliberados. Si es posible, realice copias de seguridad en un almacenamiento en línea inmutable, completamente sin conexión o fuera del sitio.

Aumente la defensa contra los ataques de ransomware

La amenaza multifacética de la nueva economía de ransomware y la naturaleza elusiva de los ataques de ransomware operados por humanos requieren que las organizaciones adopten un enfoque de seguridad integral.

Los pasos que describimos anteriormente ayudan a defenderse contra patrones de ataque comunes y ayudarán mucho en la prevención de ataques de ransomware. Para fortalecer aún más las defensas contra el ransomware operado por humanos y otras amenazas, use herramientas de seguridad que puedan proporcionar una visibilidad profunda entre dominios y capacidades de investigación unificadas.

Para obtener información general adicional sobre ransomware, completa con consejos y procedimientos recomendados para la prevención, detección y corrección, consulte Proteja su organización del ransomware, y para obtener información aún más detallada sobre el ransomware operado por humanos, lea Ransomware como servicio: comprensión de la economía por encargo de la ciberdelincuencia y cómo protegerse de Jessica Payne, investigadora de seguridad sénior.

Visite Security Insider para mantenerse al tanto de los problemas de seguridad cambiantes.

Comparta esta infografía:

Microsoft