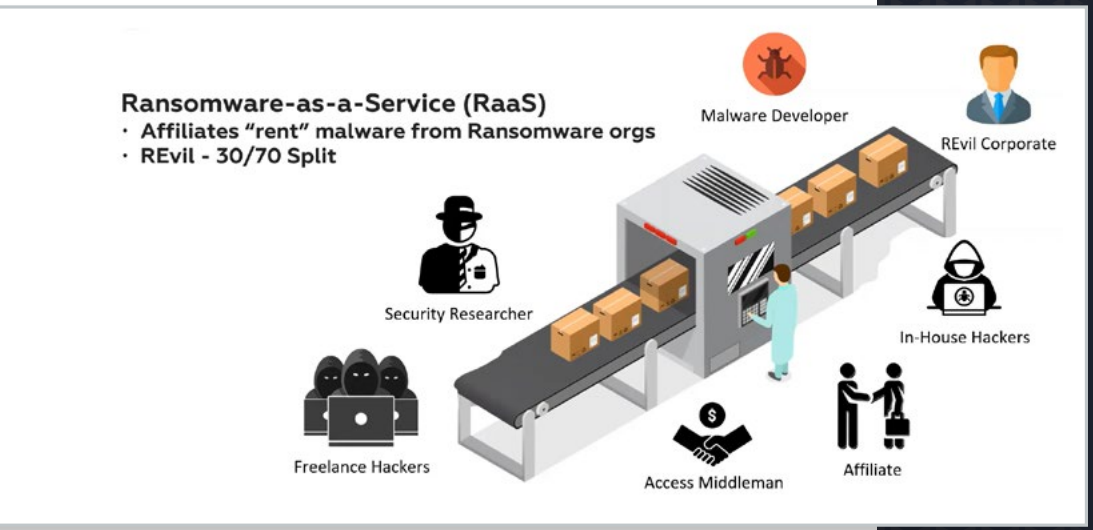
HORIZON3.ai

~~TRUST BUT~~ VERIFY

Impacto del Ransomware

con Horizon3.ai

El ransomware es un ataque cada vez más común y lucrativo, y las organizaciones a menudo pagan millones de dólares para descifrar y recuperar su información. El Informe de Investigación de Violación de Datos de Verizon (DBIR) de 2021 informó que los ataques de ransomware están en aumento, "más del doble de su frecuencia" con respecto al año anterior. Los ataques de ransomware se han democratizado, con grupos criminales que establecen operaciones de Ransomware-as-a-Service (RaaS), alquilando ransomware a afiliados reclutados que, a su vez, ejecutan ataques contra organizaciones y pagan una "regalía" a los proveedores de RaaS.



Los ataques de Ransomware están creciendo en prevalencia e impacto. ¿Qué tan malo es?

El Departamento del Tesoro de EE. UU. informó que se pagaron USD 590 millones en ransomware en la primera mitad de 2021, más que los USD 416 millones informados para todo 2020

Un estudio de 2021 realizado por Sophos encontró que el 37 % de los encuestados experimentaron ataques de ransomware. El promedio pagado por organizaciones medianas fue de USD 170,404.

El ataque de Darkside a Colonial Pipeline paralizó las operaciones hasta que la compañía pagó USD $4.4 millones.

CNA Financial, una de las compañías de seguros más grandes de los EE.UU, pagó a los hacker USD 40 millones después que un ataque de ransomware bloqueó el acceso a la red de la compañía.

Las aseguradoras que ofrecen ciber cobertura han tomado nota. AIG aumentó sus precios en un 40% globalmente. La aseguradora Optio informó una reducción del 50% en sus límites de cobertura.

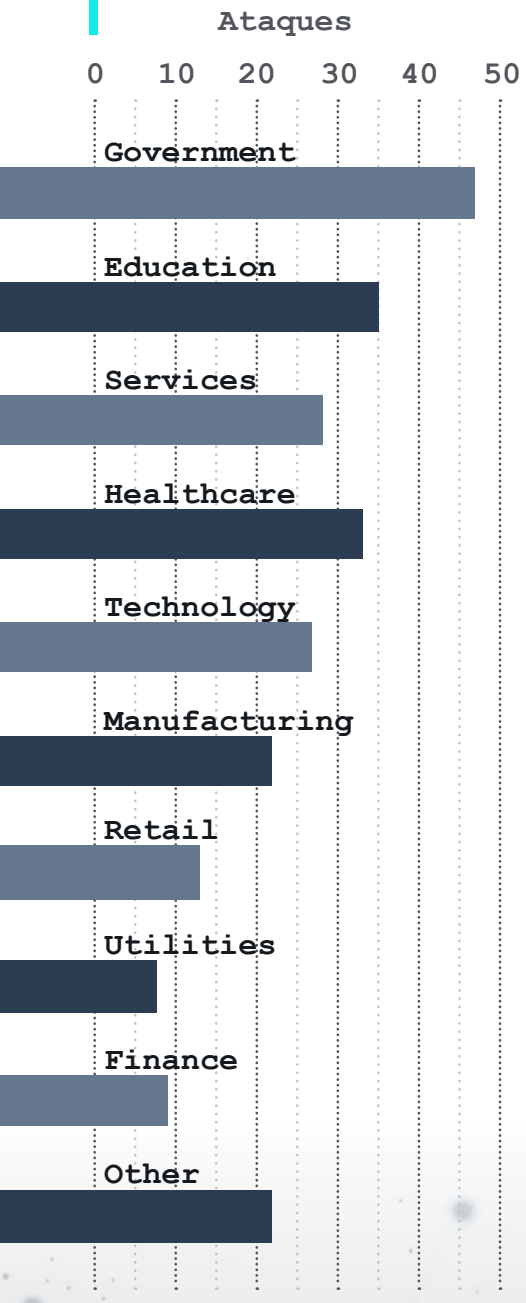
¿Cómo Funciona el Ransomware?

En un ataque ransomware, como en un ataque de robo de datos, los delincuentes se infiltran en la red de una empresa y luego se mueven lateralmente para identificar datos confidenciales. El acceso inicial a la red a menudo proviene al comprometer una credencial legítima. Sin embargo, en lugar de simplemente robar una copia de los datos, los cifran y exigen el pago en criptomonedas antes de proporcionar una clave de descifrado. Los recientes ataques del ransomware BlackMatter siguen un patrón común. Comenzando con una credencial comprometida, el ransomware realiza:

- **Enumeración de Active Directory** – Captura información que puede usarse para descubrir servidores en la red, elevar privilegios, o ayudar con movimiento lateral.
- **Enumeración SMB Compartidos** – Determina archivos compartidos a los que puede acceder con privilegios leer/escribir.
- **Descarga de Credenciales** – Identifica servidores que tienen acceso administravio y se apropian de más credenciales.
- **Encriptación de SMB Compartidos** – Esto incluye compartidos asequibles por el administrador como ADMIN$, C$, SYSVOL, NETLOGON.
- **Encriptación de Máquinas Virtuales VMware ESXi** – Los criminales extienden sus ataques a las máquinas virtuales.
- **Borrado/Reformateo** – Evita que las organizaciones hagan roll back de los sistemas para respaldar datos y aplicaciones.

Desafíos Deteniendo Ataques Ransomware

ATAQUES RANSOMWARE **POR INDUSTRIA**[9]



Como se ve los ataques de ransomware son similares a los ataques de robo de datos, pero con un tratamiento diferente de los datos (cifrado). A diferencia de ataques más sofisticados, el ransomware no depende de la persistencia a largo plazo en una red. El ataque puede ser relativamente rápido y efectivo.

Las organizaciones enfrentan varios desafíos al defenderse del ransomware, incluyendo:

- **Vector de Ataque Simple** – Los hackers de ransomware a menudo se apoyan en un ecosistema de brokers de acceso inicial que les proveen credenciales comprometidas y web shells con acceso a las organizaciones objetivo.
- **Sistemas sin protección o mal configurados asequibles para personas no autenticadas** – Para los que no compran credenciales robadas, encontrar una aplicación de cara a Internet a menudo puede permitirle poner un pie adentro.
- **Ambiente TI cambiante** – Las organizaciones cambian constantemente sus ambientes. El hosting en la nube, los proyectos TI en las sombras, y las nuevas aplicaciones cambian la superficie de ataque, dificultando a los defensores identificar, priorizar y mitigar el riesgo.
- **Exámenes de penetracion manuales no son escalables** – Los pentests pueden identificar debilidades y mejorar las defensas. Sin embargo, los pentests manuales toman tiempo, son caros e incompletos.
- **Escáneres de vulnerabilidades** – Algunos escáneres de vulnerabilidades o pentests informan hallazgos críticos de seguridad. Estos requieren analistas expertos para determinar si los hallazgos informados son ciertos positivos, falsos positivos o, lo que es peor, problemas que requieren conjuntos de condiciones obtusas y muy poco probables para explotar.

¿Cómo Ayuda Horizon3.ai?

NodeZero ayuda a las organizaciones a entender el impacto que el ransomware podría tener en sus ambientes usando las mismas tácticas y técnicas usadas por los hacker avanzados. NodeZero identifica los vectores de ataque, verifica la efectividad de cada uno, entrega una "prueba" para verificar cada debilidad (o cadena de debilidades), enumera todos los datos y servidores que podría comprometer, y entrega una guía de remediación para eliminar la amenaza. Ya que es un Servicio de Pentesting Autónomo SaaS, los pentests pueden comenzar en minutos, no en horas o días.

Reconocimiento – Al igual que APTs, ransomware, y otros actores maliciosos, NodeZero ejecuta un amplio reconocimiento para descubrir y tomar las huellas dactilares de la superficie de ataque externa e interna, identificando las formas en que las vulnerabilidades explotables, malas configuraciones, credenciales obtenidas, y valores por defecto de los productos pueden encadenarse para facilitar un compromiso.

Loop de Maniobras – NodeZero actúa como una Amenaza Persistente Avanzada (APT), orquestando más de 100 herramientas ofensivas para obtener credenciales, explotar vulnerabilidades, y explotar valores por defecto y malas configuraciones para ejecutar ataques.

Planes de Ataque Verificados – Los resultados se entregan como "Pruebas" con representaciones gráficas y textuales de cada paso de un ataque exitoso, incluyendo las tácticas usadas, cómo se obtuvieron las credenciales, las rutas seguidas para obtener privilegios y acceder a los sistemas.

Impacto – Al igual que un hacker decidido, NodeZero expone los datos en riesgo tanto en los ambientes físicos como virtuales a los que pudo acceder con privilegios de read/write, incluyendo compartidos SMB, NFS, FTP, almacenamiento en la nube, servidores vCenter, y bases de datos.

Evaluación Contextual – En vez de basarse en las puntuaciones CVSS, NodeZero evalúa cada debilidad por su rol en el ataque exitoso. Las organizaciones pueden identificar rápidamente las debilidades que representan las mayores amenazas y deben ser tratadas inmediatamente, y cuales debilidades pueden diferirse sin correr riesgo.

Remediación Accionable – NodeZero entrega una guía de remediación precisa y procesable, que permite a seguridad y operaciones resolver los problemas en su raíz.

¿Listo para aprender más?

NodeZero es un Servicio de Pentesting Autónomo SaaS que ayuda a las organizaciones a **encontrar y arreglar vectores de ataque antes que los hackers puedan explotarlos.** Es seguro correrlo en producción y no requiere agentes persistentes o acreditados.

Solicite hoy su demo gratuita.

FUENTES DEL ARTICULO [N] - https://www.horizon3.ai/ransomware-impact-sources

  @Horizon3ai info@horizon3.ai www.horizon3.ai

HORIZON3.ai
~~TRUST~~ BUT VERIFY