BOLETÍN DE ALERTA

Boletín Nro.: 2020-28

Fecha de publicación: 15/09/2020

Tema: Ransomware-as-a-Service (RaaS) combinado con técnicas de intrusión a redes.

Descripción:

Se ha visto recientemente, un cambio en la tendencia de ataques con ransomware a organizaciones públicas y privadas en la región.

Los grupos de ciberdelincuentes no solo optan por los métodos tradicionales para infectar con ransomware a un sistema, como lo es por ejemplo el phishing o la ingeniería social, sino que pasaron de ser ataques genéricos, automatizados, basado en el volumen en la cantidad de víctimas, a ser ataques dirigidos a organizaciones específicas, con técnicas de intrusión a redes, muchas veces, manuales y personalizadas, que incluyen no solo el acceso inicial, sino también técnicas de movimiento lateral, análisis minucioso de la red, propagación a través de la red para finalmente implantar el ransomware en sistemas estratégicos y logrando así eludir también potenciales **defensas de seguridad** para finalmente difundir el ransomware en la red afectada, asegurando el máximo impacto.

En este boletín se introduce especialmente el concepto de **técnicas de movimiento lateral**, las cuales son utilizadas por ciberdelincuentes después de un posterior acceso a los sistemas, todo esto con el fin de lograr mayor nivel de intrusión en la red y finalmente implantar el ransomware en posiciones estratégicas de la red afectada.

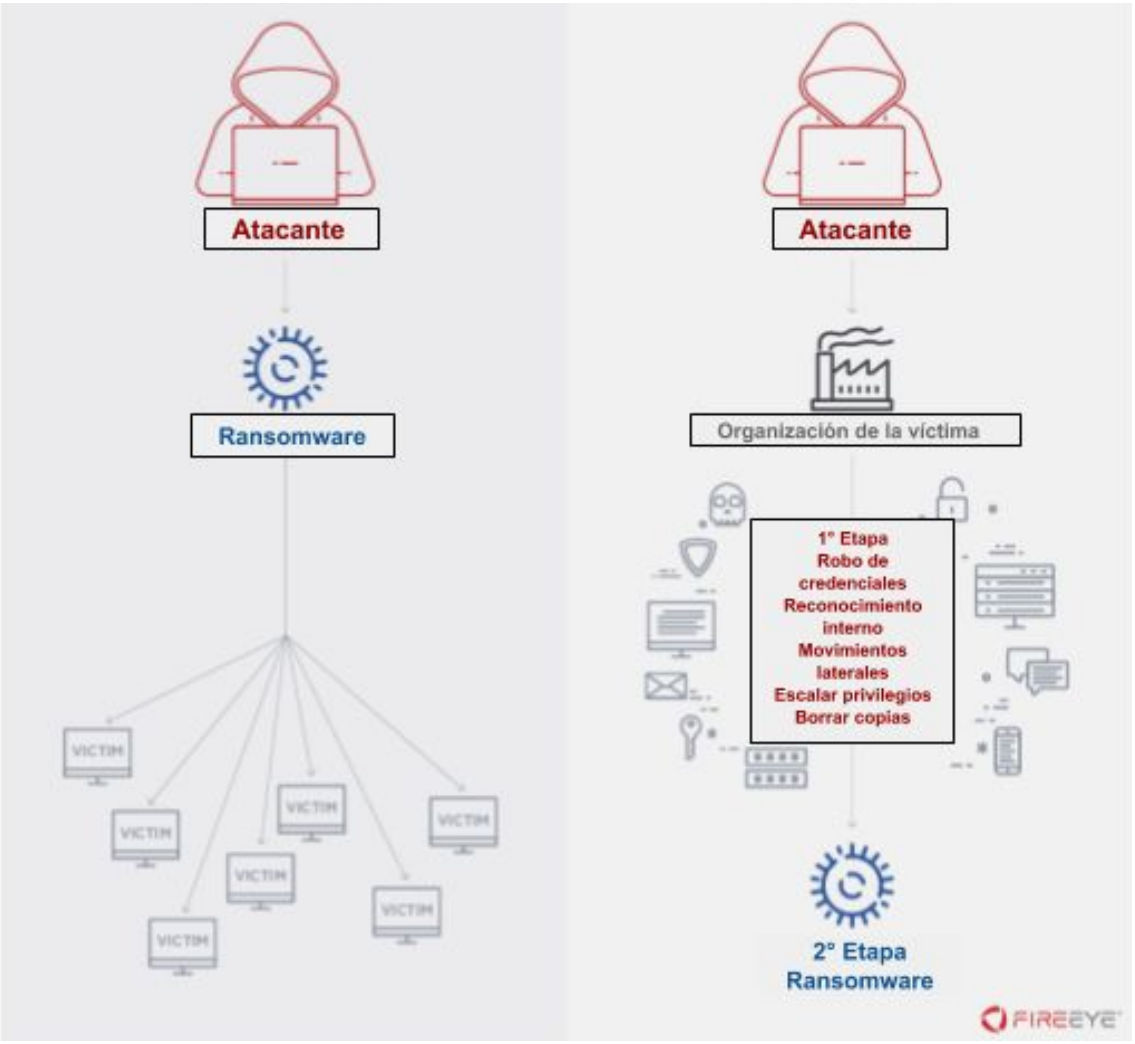
Algunas de las técnicas y herramientas de movimiento lateral utilizadas por los ciberdelincuentes son:

- **Pass the Hash**, permite a un ciberdelincuente utilizar el **hash LM** (LAN Manager) **y NTLM (New Technology LAN Manager)** para autenticarse a un servidor o servicios remotos a través de **SMB (Server Message Block).**
- **Pass the ticket**, método utilizado para autenticarse en el sistema utilizando **tickets de Kerberos** sin necesidad de contar con acceso a la contraseña de la víctima y acceder a los recursos para los cuales éste tenga permiso.

- La **herramienta Psexec**, utilizada por administradores para controlar remotamente los sistemas Windows desde la interfaz de línea de comandos. Resulta interesante para los ciberdelincuentes debido a la capacidad que tiene de cargar, ejecutar e interactuar con un ejecutable en un host remoto, además no alerta al usuario remoto de su funcionamiento ya que se trata de una herramienta legítima de administración de sistemas.
- La **herramienta Mimikatz**, utilizada principalmente para obtener contraseñas en texto plano, hashes y para la generación de tickets de Kerberos desde la memoria.
- **Powershell**, utilizada por ciberdelincuentes para obtener credenciales en la memoria, modificar configuraciones del sistema y automatizar el movimiento de un sistema a otro.
- El **escaneo de puertos**, técnica simple utilizada para identificar los servicios de interés, como aplicaciones web o servidores de bases de datos y la funcionalidad de acceso remoto. Si bien un escaneo es fácil de detectar, los escaneos “bajos y lentos” podrían superar cualquier sistema de monitoreo de red.
- Explotación de vulnerabilidades, existen casos en los cuales los ciberdelincuentes aprovechan vulnerabilidades conocidas para lograr el movimiento lateral en la red (por ejemplo: CVE-2019-2725, CVE-2018-8453).

Podemos resumir que, el objetivo principal de los ciberdelincuentes es lograr obtener la cantidad máxima de información sobre el sistema vulnerado, mediante un reconocimiento interno luego de la intrusión, obtener credenciales de acceso u otra información potencialmente útil, para luego mediante técnicas de movimiento lateral buscar la propagación del ransomware asegurándose de que sea un daño importante y que la intrusión pase desapercibida hasta tanto el ransomware esté estratégicamente implantado.

Además es importante recordar que ransomwares como **Maze, Clop, DoppelPaymer, Nefilim, Sekhmet, Robin Hood y Nemty**, utilizan la exfiltración de datos antes de implantar el código malicioso, es decir, roban datos potencialmente confidenciales de la víctima u organización para seguidamente hacerlos públicos o comercializarlos en la dark web.



Fuente: FireEye

Algunos casos en los que fueron aplicadas estas metodologías de ataque:

El ataque del ransomware **WastedLocker** dirigido a la **empresa Garmin**, donde los ciberdelincuentes realizaron un primer intento de intrusión, para evaluar el sistema de defensas y posteriormente diseñar un ataque específico para eludir el software de seguridad, dicho ataque forzó a los empleados de la compañía a apagar sus dispositivos para no quedar

infectados. Para más información puede ver el siguiente enlace.

El incidente de seguridad en la **empresa Pitney Bowes**, donde los ciberdelincuentes publicaron datos sensibles de la compañía luego de la infección con el **ransomware Maze** expandiendo el acceso del malware a todos los sistemas internos posibles. Para más información puede ver el siguiente enlace.

Un **condado de Los Ángeles** fue afectado por el ransomware **DoppelPaymer**, en donde los ciberdelincuentes afirmaron haber accedido y encriptado un total de **150 servidores** y **500 estaciones de trabajo**, para obtener más de **200GB de archivos.** Para más información puede ver el siguiente enlace.

El **ransomware REvil** atacó a la **fábrica de Jack Daniel's**, en este caso la compañía pudo intervenir antes de que los sistemas fuesen encriptados, pero no pudieron averiguar cuándo tuvo lugar el ataque, en reportes se estimó que los ciberdelincuentes tuvieron acceso al sistema por más de un mes y afirmaron haber robado más de **1 TB** de datos de la compañía. Para más información puede ver el siguiente enlace.

Uno de los casos más recientes con el **ransomware REvil** fue el del **Banco Estado de Chile**, en donde a través de un comunicado de prensa informó que todas las sucursales se encontrarán inoperativas y cerradas mientras solucionan el problema ocurrido. Los ciberdelincuentes obtuvieron acceso a la plataforma del banco mediante ataques del tipo APT (Amenaza Avanzada Persistente) y estudiaron el ambiente durante un tiempo antes de realizar la infección con el ransomware.

El caso de la banda del **ransomware Netwalker**, la cual pasó de ser una banda "genérica" a contratar ciberdelincuentes expertos en **intrusión de red** capaces de analizar su entorno y escalar el acceso. Fijando con esto, como único objetivo principal a las grandes empresas, evitando toda campaña de phishing masiva y centrándose en ataques con técnicas avanzadas de intrusión de redes, adoptando un nuevo "**modelo de negocio RaaS**", al igual que otros como el **ransomware Sodinokibi/REvil**.

Impacto:

Un ataque exitoso a la red podría generar daños como:

- Pérdida de datos confidenciales y críticos almacenados en el disco o copias de seguridad
- Interrupción de las actividades regulares y un daño importante a la reputación de la organización
- Pérdidas financieras considerables, durante la restauración de los sistemas afectados
- Robo de datos y exfiltración de los mismos a un servidor controlado por los ciberdelincuentes, para utilizarlo como método de extorsión o para su publicación en la dark web.

Solución y prevención:

- Realizar monitoreos activos frecuentes, preferentemente continuos de la red interna a nivel de tráfico con herramientas de detección de intrusos y monitoreo de red, esto con el fin de determinar si existen anomalías de fugas de información del tráfico de la red interna hacia afuera. Configurar alertas personalizadas que puedan notificar a los administradores de red cuando una anomalía se produzca.
- Configurar las herramientas de seguridad para detectar, alertar y bloquear la presencia de técnicas y herramientas específicas como PsExec, Mimikatz y eventos específicos de movimiento lateral. Para más información consultar los siguientes enlaces:
    - https://medium.com/@imphash/detecting-lateral-movement-101-tracking-movement-smb-windows-admin-shares-through-windows-log-6005e3ba6980
    - https://resources.infosecinstitute.com/advance-persistent-threat-lateral-movement-detection-windows-infrastructure-part/#gref
    - https://www.trendmicro.se/media/wp/detecting-apt-activity-with-network-traffic-analysis-whitepaper-en.pdf
- Utilizar **Sistemas de Prevención de Intrusos (IPS)**, los cuales cuentan con la función

principal de identificar, bloquear y prevenir actividades maliciosas mediante patrones específicos de ataque en el tráfico de red. Estos sistemas pueden utilizar algunos de los siguientes metodos de deteccion:

- **Basado en firmas**, en este caso, se analizan los paquetes de la red y se comparan con patrones de red conocidos y preconfigurados, dichos patrones se denominan “firmas” y se encuentran almacenados en una base datos que debe ser actualizada periódicamente.
- **Basado en anomalías**, determina la actividad normal de la red, como el orden de ancho de banda utilizado, protocolos y puertos generalmente interconectados y, en caso de que lo considerado como normal varía, alerta al administrador o usuario clasificandolo como anómalo.
- **Basado en análisis de protocolo**, similar al basado en firmas, pero en este caso se realizan inspecciones mucho más profundas en los paquetes y además tienen la posibilidad de encontrar más fácil algunos tipos de ataques.

- Limitar la distribución de cuentas privilegiadas y monitorear el uso de credenciales privilegiadas en tiempo real, esto para detectar potenciales movimientos laterales en la red. Es recomendable establecer alertas a los administradores sobre el acceso a servidores críticos, como así también configurar alertas ante la creación de usuarios nuevos en el directorio activo.
- Permitir únicamente que aplicaciones legítimas sean ejecutadas en la red y además registrar todos los intentos de inicio de otras aplicaciones. Esta “lista blanca” de aplicaciones no es una solución infalible, sin embargo, puede ayudar en la detección de potenciales intrusos en la red.
- Crear contraseñas seguras mediante el uso de protocolos de contraseña automatizados. Utilizar el factor doble de autenticación en los sistemas que lo admitan y especialmente en aplicaciones web con conexión a internet.
- Mantener los sistemas y dispositivos actualizados con los últimos parches de seguridad, para evitar que potenciales ciberdelincuentes tomen provecho de vulnerabilidades para atacar al sistema.
- Manejar con cuidado la información sensible compartida en la red, utilizar herramientas que ayuden a la configuración de permisos de acceso en carpetas compartidas y dentro del sistema de archivos de la empresa.

- Controlar los puertos abiertos en la red con frecuencia y bloquear aquellos que no sean utilizados, esta configuración puede implementarse por reglas de GPO (Directivas de Grupo) en Windows o bien a través de políticas en las consolas de administración de soluciones IPS/IDS.
- Asegurar que la red se encuentra segmentada de forma que desde un sistema no sea posible acceder a otro, es decir, evitar que la totalidad de la red informática sea accesible desde un mismo punto, esto podría realizarse mediante el uso de VLANs (red de Área Local Virtual) o subnetting (creación de subredes pequeñas dentro de una más grande).
- Concientizar a los usuarios a descargar archivos únicamente de sitios de confianza.
- Habilitar un firewall para evitar accesos no autorizados a la red, tanto a nivel de red como especialmente a nivel de host, limitando no solo el tráfico entrante sino también el tráfico entre equipos de un mismo segmento y entre segmento. Asegurar que las reglas permitan única y exclusivamente las conexiones estrictamente necesarias (entrantes y salientes).
- Realizar una auditoría de los protocolos como RDP, SMB, SSH, FTP y recursos compartidos en la red, deshabilitar los protocolos que no son utilizados y además eliminar unidades compartidas innecesarias, todo esto para evitar la difusión de malware en la red.
- Prestar atención con el aseguramiento de las copias de seguridad, identificando claramente los datos críticos para las operaciones normales de la organización y asegurando que dichas copias de seguridad críticas sean almacenadas también de manera offline, o mínimamente en una red separada.

Información adicional:

- https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
- https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html

- https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html
- https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html
- https://threatpost.com/la-county-hit-with-doppelpaymer-ransomware-attack/155024/
- https://www.xataka.com/seguridad/wastedlocker-asi-actua-nuevo-ransomware-evil-corp-detras-ciberataque-a-garmin
- https://www.insurancejournal.com/news/international/2020/04/14/564766.htm
- https://grupooruss.com/conoces-los-ataques-laterales%E2%80%8B-del-hacking/
- https://www.ciberseguridadlogitek.com/movimientos-laterales-mejores-practicas-para-proteger-tu-red/
- https://www.sophos.com/es-es/security-news-trends/best-practices/10-tips.aspx