Ataques contra el ransomware en el 2020 - ¿Cómo sobrevivir en el 2021?

RIDGE SECURITY

El uso de RidgeBot para obtener una solución de seguridad basada en los riesgos de la empresa

Ataques contra el ransomware en el 2020 - ¿Cómo sobrevivir en el 2021?

Un ataque de ransomware es una forma de extorsión, y los sobornos han aumentado drásticamente en 2020. A menudo parecía que cada dos días salían noticias de algún lugar del mundo sobre otra empresa afectada por un ataque de ransomware que provocaba consecuencias devastadoras, extorsiones y pagos cada vez mayores.

En el 2020, el ransomware produjo suficientes daños como para consolidar su posición como una amenaza para en una sala de reuniones. Los ataques van en aumento en todos los aspectos.

- Número de víctimas
- Número de pagos
- Importe de los pagos
- El daño a las organizaciones
- La extorsión por los datos robados, además del rescate por desencriptar los datos

Blackfog informa que " los ciberataques de ransomware son un gran negocio... Las investigaciones anticipan que una empresa es atacada por un ciberdelincuente cada 11 segundos y el costo de los daños causados por estos ataques alcanzará alrededor de $20 mil millones para 2021." Un ataque al Hospital Universitario de Düsseldorf, en Alemania, en septiembre de 2020, se saldó con la pérdida de vidas humanas, ya que un paciente de urgencia tuvo que ser desviado a otro centro y no pudo ser atendido a tiempo.

Tendencias de ransomware

Varias tendencias están generando un rápido aumento tanto de la frecuencia como del tamaño de los ataques en el 2020. Los actores de las amenazas también están modificando su estrategia para obtener pagos más grandes y seguros.

Tendencias que fomentan el aumento en la incidencia de los ataques de ransomware

Las actividades y las tendencias de la industria han aumentado drásticamente la posibilidad de que las redes tanto de las pequeñas como grandes compañías y administraciones públicas sean objeto de ataques. Otras tendencias también han abierto nuevas oportunidades.

- **Migración a la nube:** La tecnología basada en la nube ha crecido rápidamente en los últimos años, proporcionando un importante ahorro de costos y agilidad empresarial a organizaciones de todos los tamaños. Las plataformas y los servicios en la nube ofrecen a las empresas una flexibilidad mucho mayor en cuanto al almacenamiento, la computación y las necesidades de crecimiento y reducción con tarifas de pago por uso en lugar de una fuerte inversión en infraestructura de hardware.
- **El Covid-19, pandemia y trabajo desde casa:** la respuesta global a la pandemia ha provocado un cambio trascendental y repentino en la mayoría de los profesionales con trabajo desde casa: La respuesta global a la pandemia provocó un cambio trascendental y repentino hacia una fuerza de trabajo profesional mayoritariamente desde cualquier lugar (WFA). Los esfuerzos urgentes de las organizaciones para mantener la continuidad del negocio durante el aislamientos por Covid-19 aceleraron además la ya fuerte tendencia a la migración a la nube. Juntas, las tendencias de la nube y la WFA han disuelto el tradicional perímetro rígido de la red empresarial, sustituyéndolo por un perímetro definido por software (SDP) que recorre cada superficie de la red abierta al acceso a Internet. Las empresas están luchando con las capacidades y tecnologías siempre cambiantes para asegurar adecuadamente este nuevo perímetro blando y el acceso WFA a través de Internet.
- **IoT:** Los dispositivos de bajo costo no gestionados se están multiplicando en las redes para automatizar, observar, informar, medir, supervisar y vigilar una amplia gama de dispositivos y situaciones de consumo y comerciales, desde el sector industrial hasta el agropecuario. Los dispositivos IoT suelen utilizar copias obsoletas de pilas TCP/IP de código abierto, carecen incluso de capacidades de seguridad rudimentarias y no ofrecen ninguna metodología para rastrear o instalar parches para las vulnerabilidades conocidas.

Otras tendencias más específicas del ransomware también han provocado un aumento significativo de la complejidad, la importancia y la eficacia financiera de los ataques.

- **Ransomware-as-a-Service (RaaS):** En el pasado, los objetivos de los ataques eran naturalmente limitados porque sólo unos pocos delincuentes altamente cualificados tenían la infraestructura, la capacidad técnica y la metodología de ejecución afinada para infiltrarse en las redes bien protegidas de las grandes organizaciones.

  Siguiendo el mismo camino de facilidad de despliegue con habilidades limitadas que SaaS, IaaS y PaaS han capitalizado, RaaS también se ha trasladado a la nube, donde los kits de ransomware altamente personalizables, comprados en la web oscura, pueden desplegarse con facilidad. Esto ha rebajado el listón de entrada y ha permitido a una población mucho mayor de actores de amenazas lanzar ataques sofisticados. RaaS ofrece diferentes tipos de programas de socios afiliados, con un portal web completo en el que los afiliados pueden obtener kits actualizados. REvil/Sodinokibi y Netwalker son ejemplos que utilizan un modelo RaaS.

- **Spam y phishing:** Este ha sido durante mucho tiempo el punto de acceso más exitoso para el malware, pero la pandemia de Covid-19 ha acelerado esta tendencia con muchas nuevas oportunidades aprovechando el miedo humano así como explotando las vulnerabilidades abiertas por las configuraciones de WFA. Los actores de la amenaza se hacen pasar por organizaciones que proporcionan información sobre el Covid-19, estadísticas, programas gubernamentales de ayuda económica, equipos de protección personal o información sobre vacunas.

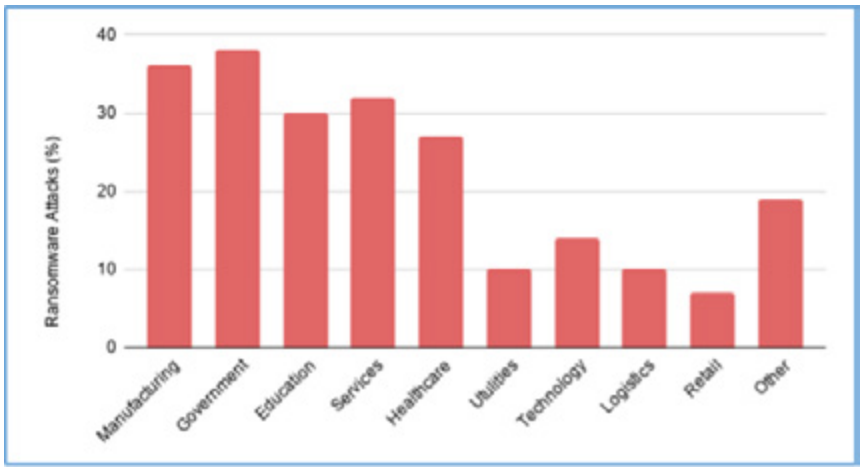
- **Pagos con Bitcoin:** La creciente popularidad y disponibilidad de criptomonedas como el bitcoin ofrecen métodos de pago sin trazabilidad, sin opción de disputa y con transacciones no cancelables.

Tendencias en los métodos de ataque del ransomware

El ransomware sigue dirigiéndose ocasionalmente a los consumidores, pero la mayor parte de los ataques han pasado a **centrarse en objetivos corporativos y gubernamentales**. La filtración inicial de activos es casi tan fácil y las oportunidades de pago son enormes.

En el 2020, los actores de las amenazas han apuntado específicamente a las grandes organizaciones, y a menudo a aquellas con una **exposición legal**. La perspectiva de las multas reglamentarias y el daño a la reputación resultante de las violaciones de la privacidad de los datos expuestas públicamente aumentaron significativamente la tasa de éxito de los pagos, así como los importes de los mismos.

SOCRadar Labs informa de que los sectores más afectados por el ransomware en el 2020 son el sector industrial, la administración pública y los proveedores de servicios profesionales; organizaciones especialmente reacias al tiempo de inactividad.



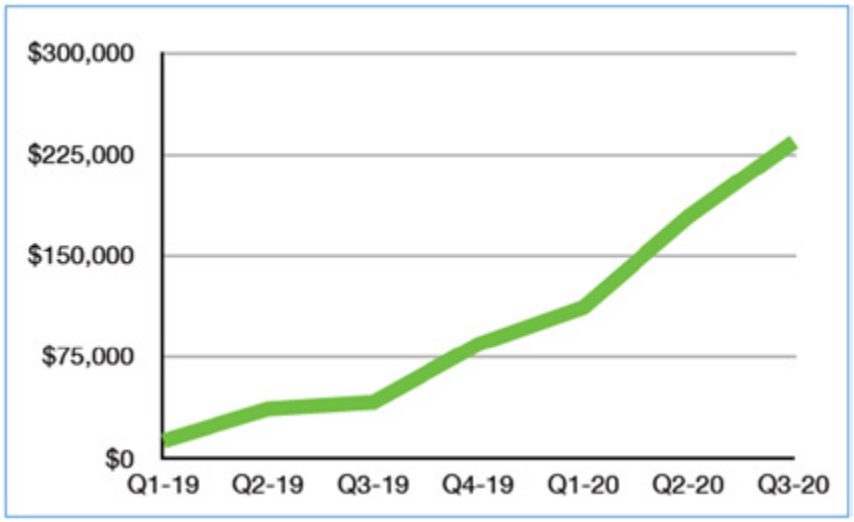
El ransomware ha experimentado un considerable **aumento de la virulencia** y, gracias a RaaS, **una mayor población de actores** de amenazas que pueden dirigirse a un mayor número de víctimas.

Además de simplemente pedir un rescate por los datos de una organización mediante el cifrado, un número cada vez mayor de los ataques más recientes **combina el cifrado con la extorsión** para aumentar la probabilidad de un pago. En estos ataques combinados, el actor de la amenaza primero obtiene acceso a los activos de la organización y exfiltra sus datos, y sólo entonces los cifra. Si la organización se niega a pagar por la clave de descifrado, el actor de la amenaza expone los datos exfiltrados poniéndolos a disposición del público o subastándolos en la web oscura, dañando así la reputación y el bienestar financiero de la organización.

Esta tendencia hace que los ataques de ransomware se conviertan también en violaciones de datos. También obliga a la gestión de la seguridad de las organizaciones a reevaluar el riesgo y la respuesta a los incidentes, y a ajustar las estrategias de recuperación de desastres y de continuidad del negocio. Los grupos de ransomware siguen aprovechando esta táctica de exfiltración de datos y extorsión, aunque la confianza en que los datos robados serán eliminados se está erosionando, ya que el incumplimiento de las promesas es cada vez más frecuente a pesar de que la víctima pague el rescate.

Los actores de las amenazas también han aprovechado el hecho de que las **empresas se encuentran distraídas por la pandemia del Covid-19**. Mientras se lleva a cabo una reingeniería de emergencia de la red y la informática para garantizar la continuidad del negocio, las vulnerabilidades de seguridad expuestas por las migraciones a la nube y la WFA a menudo permanecen sin resolver durante un período de tiempo. La proliferación de configuraciones WFA que utilizan RDP y otras tecnologías de acceso remoto permiten a los actores de las amenazas aprovechar vectores de ataque que antes no existían.

En los últimos dos años, el **promedio de pago de rescates** también ha aumentado significativamente, como se muestra en el Informe Mensual de Ransomware de Blackfog. Este aumento se atribuye en parte a que los atacantes se dirigen cada vez más a las grandes empresas.



Geográficamente, los ataques de ransomware se dirigen sobre todo a **Asia, América del Norte y Europa**, aunque ningún país u organización del mundo está exento.

Tradicionalmente, los actores de las amenazas han apuntado a los sistemas Windows por ser la mayor base de **sistemas operativos instalados**, pero como los sistemas MacOS han ganado cuota de mercado en los últimos tiempos, estas plataformas también son cada vez más atacadas.

Un informe de mercado de Coveware indica las estadísticas del tercer trimestre de 2020 de los 10 principales tipos de ransomware.

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2020
1	Sodinokibi	16.2%	-
2	Maze	13.6%	-
3	Netwalker	9.9%	+1
4	Phobos	5.0%	-2
5	DopplePaymer	4.3%	New in Top 10
6	Snatch	4.0%	+2
6	Conti	4.0%	New in Top 10
8	Lockbit	3.6%	+1
9	Dharma	2.3%	-4
10	Nephilim	2.0%	New in Top 10
10	Avaddon	2.0%	New in Top 10

Tendencias en el manejo de los ransomware

Los presentadores de Mandiant/FireEye en el evento virtual de BlackHat Europe, celebrado en diciembre de 2020, hablaron de las mejoras y los cambios en el comercio de ransomware que observaron en 2020.

- Más sigilo, menos ruido: los ataques de ransomware son rápidos, pero ruidosos
- Mejora de las herramientas: menos dependencia de las herramientas estándar de pruebas de penetración y uso de más malware a medida.
- Mayor rapidez en la obtención de credenciales de administrador de dominio
- Mejora de los métodos de despliegue del ransomware
- Mayor eficacia para eliminar las copias de seguridad

Acciones recomendadas de mitigación

Incluso el ataque más sencillo puede hacer que una organización pierda mucho tiempo y dinero. Los ataques sofisticados, y los ataques combinados de extorsión y encriptación, pueden causar un golpe demoledor o destruir por completo una empresa. Las recomendaciones generales para minimizar los daños de un ataque de ransomware incluyen:

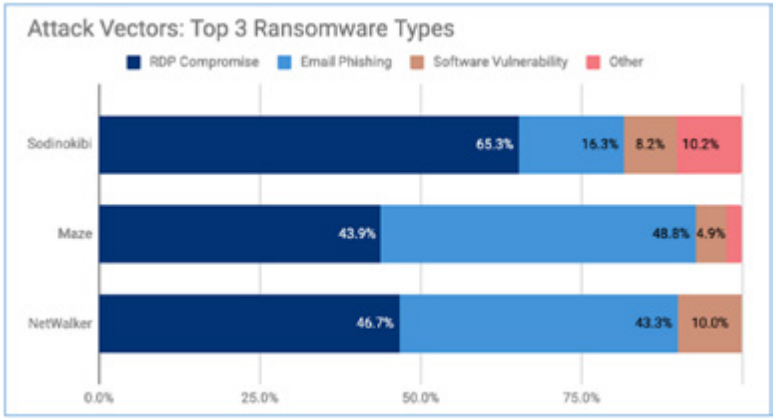
- Establecer y mantener copias de seguridad fuera de línea, y probarlas regularmente para garantizar que los sistemas puedan reconstruirse con éxito.
- Instruir a los empleados sobre estrategias de ingeniería industrial y phishing.
- Establecer una estrategia para evitar el robo no autorizado de datos, especialmente cuando se almacenan o suben grandes cantidades de datos a plataformas en la nube.
- Establezca un análisis del comportamiento de los usuarios para supervisar e identificar posibles incidentes de seguridad.
- Utilizar la autenticación multifactor (MFA) en todos los puntos de acceso remoto.
- Implantar pruebas de penetración regulares o continuas para identificar los puntos débiles, las credenciales débiles y las vulnerabilidades explotadas con frecuencia.
- Desplegar tecnologías de borde de servicio de acceso seguro (SASE) para bloquear el perímetro blando (SDP) alrededor de los activos en la nube, la DIA en las oficinas y el acceso de los empleados de la WFA.
- Acciones específicas para mitigar las vulnerabilidades de la pila de protocolos TCP/IP (tanto para los activos normales de la empresa como para el IoT): desactivar el IPv6 cuando/donde no sea necesario; confiar en los servidores DNS internos para los dispositivos críticos; supervisar su red para detectar paquetes y comportamientos anómalos; segmentar su red para evitar el movimiento lateral del malware.
- Desconfíe de los servicios expuestos públicamente, como el Escritorio Remoto (RDP, puerto 3389), la VPN, la Computación de Red Virtual (VNC), el FTP y el Bloqueo de Mensajes del Servidor (puerto 445).
- No instales software ni le des privilegios de administrador a menos que sepas exactamente lo que hace.
- Asegúrate de que todos los sistemas operativos tienen parches actualizados e instala software antivirus en todas partes.

Técnicas y fases de uso común

La mayoría de los ataques de ransomware utilizan un pequeño número de vectores de infecciones comunes.

- **Phishing:** Archivos adjuntos de correo electrónico maliciosos, también denominados “malspam”.
- **Protocolo de escritorio remoto (RDP):** Intrusión en la red a través de puertos y servicios no seguros.
- **Vulnerabilidades de software y de red:** Virus y otras formas de ransomware que aprovechan las vulnerabilidades de la red.
- **Malware doble:** Malware adicional introducido a través de infecciones de malware anteriores (por ejemplo, una infección de TrickBot que lleva a una infección posterior de Ryuk).

Un informe de Coveware del tercer trimestre de 2020 ofrece detalles sobre los vectores de infección de los distintos tipos de ransomware.



Las tácticas y técnicas habituales utilizadas por los autores y operadores de ransomware se dividen en varias categorías.

- **Oportunistas:** El modelo operativo de los actores oportunistas es el ransomware autopropagado, como WannaCry. Los actores de la amenaza inician el malware -a menudo utilizando puntos de entrada de fácil acceso como kits de exploits, backdoors, puertos abiertos, VPNs inseguras, sistemas operativos y aplicaciones que carecen de parches- pero después depende de las acciones de los usuarios para propagarlo y los actores de la amenaza no saben a dónde va, a dónde se va a mover, qué organización objetivo puede ser víctima, o a qué dominios o redes puede acceder.

  A veces denominados “spray-and-pray”, se trata de ataques de gran volumen y menos sofisticados, y es un método operativo que ha disminuido recientemente.

- **Dirigida:** Se trata de una técnica estratégica de menor volumen, más sofisticada, que da lugar a pagos promedio más elevados. Los actores de la amenaza utilizan una campaña específica para dirigirse a una organización concreta. Consiguen acceder a la red a través de correos electrónicos de phishing, ingeniería industrial, vulnerabilidades del sistema operativo o de puertos abiertos, y luego buscan en la red antes de desatar sus demandas de rescate. Hay dos modos de funcionamiento en esta técnica "dirigida":
  - **Modelo partnership:** Los "autores de amenazas" profesionales crean el ransomware y luego proporcionan a los afiliados (mediante suscripción o porcentaje del rescate) una plataforma en la que pueden acceder a herramientas e instrucciones para ejecutar los ataques. Este modelo ofrece una baja barrera de entrada para ataques muy sofisticados.

    Otro modo de operar en este modelo es cuando los "autores de la amenaza" crean el ransomware y también perpetran el compromiso inicial de la organización objetivo, y luego venden el acceso a los afiliados para ejecutar el ataque.
  - **Modelo autogestionado:** En este modo de operación los actores de la amenaza ejecutan la fase inicial de compromiso por sí mismos, obtienen acceso al sistema y al entorno, y luego se desplazan antes de ejecutar las demandas de rescate.

Proteja sus activos frente al ransomware con Ridgebot 3.2

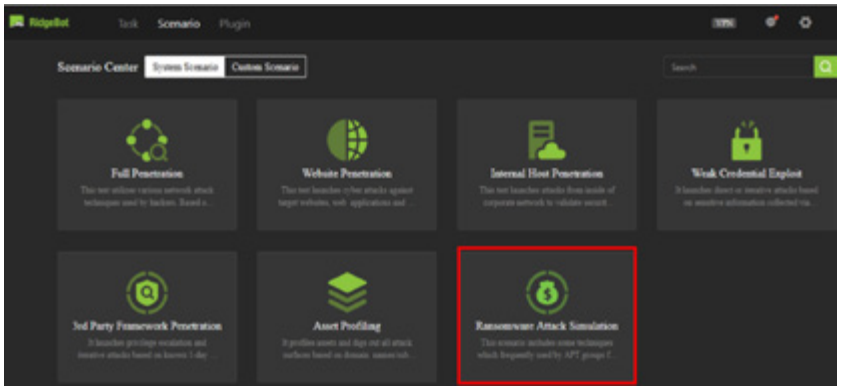
RidgeBot descubre automáticamente sus activos, los escanea y luego procede a explotar las vulnerabilidades encontradas tal como lo haría un hacker. En su informe, le avisa de las vulnerabilidades peligrosas explotadas con éxito y también le muestra la ruta de ataque exacta que permitió que el activo se viera comprometido. Con esta información detallada y precisa puede cerrar rápida y proactivamente todas las vulnerabilidades de su red y otros activos.

Protección contra el ransomware RidgeBot 3.2

La versión 3.2 incluye una nueva plantilla centrada específicamente en la lucha contra los ataques de ransomware. Inicialmente esta plantilla incluye:

- Escaneo de 27 vulnerabilidades de punto de entrada de ransomware de alto perfil
- La capacidad de lanzar ataques para explotar estas vulnerabilidades
- Informes detallados sobre la forma exacta en que se lograron las explotaciones exitosas

Con el tiempo se añadirán definiciones de más ataques de ransomware, y usted puede añadirlas a su arsenal de seguridad descargando las actualizaciones periódicas de RidgeBot.



La implementación de la plantilla de ransomware de RidgeBot 3.2 le permite lanzar rápida y fácilmente un escaneo de activos para detectar las vulnerabilidades relacionadas con el ransomware que puedan estar presentes en sus activos. Como parte integral del escaneo, RidgeBot también lanza ataques para probar que las vulnerabilidades encontradas son realmente explotables en su entorno actual. Puede ejecutar estas pruebas de penetración y ataques bajo demanda o en un horario regular.

Al igual que con otras herramientas y pruebas de vulnerabilidad, se recomienda reejecutar una exploración y explotación de plantillas de ransomware cada vez que se produzca algún cambio en sus activos, como la adición de un nuevo servidor o dispositivo de red, la actualización de software de un dispositivo, la instalación de un parche en un dispositivo, el cambio de secuencias de comandos o información en un servidor web, o cualquier otro cambio de software o hardware que pueda dar lugar a la implementación de una nueva vulnerabilidad en su red. Debe estar especialmente atento a los dispositivos IoT que puedan conectarse o insertarse en su red.

El enfoque de RidgeBot 3.2

La plantilla del ransomware de RidgeBot 3.2 incluye la exploración y explotación de las siguientes clases de vulnerabilidades:

- Ejecución remota de código/comando (RCE)
- Relleno de contraseñas y credenciales débiles (por ejemplo, SSH, Redis y SQL Server)
- Bloque de mensajes del servidor (SMB)
- WebLogic y otras cargas de archivos

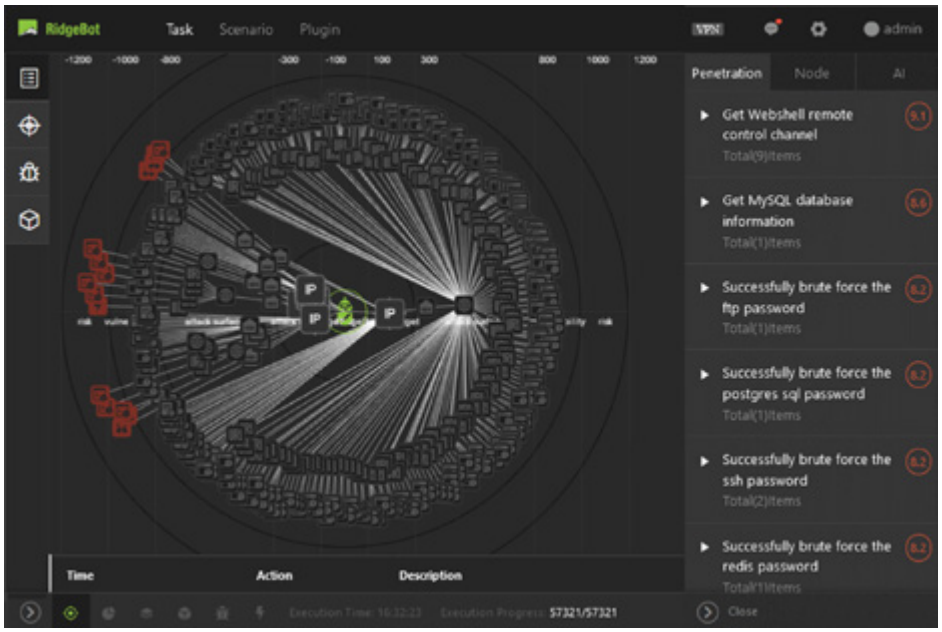
Alcance de RidgeBot 3.2

El escaneo y la explotación de RidgeBot cubren vulnerabilidades técnicas como credenciales débiles, puertos abiertos, cargas de archivos, vulnerabilidades de aplicaciones web de WebLogic y Struts2. No puede protegerle contra la ingeniería social o el phishing, ni con los datos que ya han sido cifrados por un ataque de ransomware. En su lugar, utilice RidgeBot para localizar las vulnerabilidades de su red y evitar la intrusión de ransomware.

Si considera que su organización es un “objetivo” posible o probable para los actores de amenazas, utilice las capacidades de exploración y explotación de RidgeBot 3.2 para protegerse contra la etapa inicial de compromiso de un ataque planificado. Una vez que un actor de la amenaza ha entrado en su red y ha establecido un punto de apoyo, necesitará herramientas adicionales para detectar y corregir la intrusión.

Cómo combatir los ataques de ransomware de alto perfil con RidgeBot

RidgeBot desarrolla una estructura de red de los activos descubiertos y muestra una lista de objetivos (cuadros rojos en el gráfico), y de exploits y vulnerabilidades (listados en la parte derecha de la pantalla), que fueron penetrados con éxito. Al resaltar cualquiera de estas penetraciones se revela la ruta de ataque exacta que siguió RidgeBot para comprometer ese objetivo. Esto le proporciona información clara y precisa sobre qué dispositivos de su entorno requieren qué tipos de correcciones o actualizaciones para estar debidamente protegidos contra los ataques de ransomware.



Las secciones siguientes proporcionan detalles y ejemplos de una serie de vulnerabilidades de alto perfil y fácilmente explotables que pueden existir en su entorno. RidgeBot 3.2 puede protegerle contra estas vulnerabilidades y otras más.

La agencia gubernamental estadounidense National Institute of Standards and Technology (NIST) mantiene una base de datos nacional de vulnerabilidades (NVD) en la que se pueden buscar detalles adicionales de todas las vulnerabilidades con números CVE asignados.

Ejecución remota de código/comando: EternalBlue

Los ataques masivos de ransomware a nivel mundial de 2017 fueron noticia en todo el mundo, paralizaron empresas durante varios días y costaron a varias organizaciones multinacionales millones de dólares en daños, reparaciones y recuperación. El ransomware WannaCry, que golpeó en mayo de 2017, utilizó la vulnerabilidad EternalBlue para explotar ordenadores Windows sin parches. A este le siguió, en junio de 2017, el ataque del ransomware NotPetya, que aprovechó la misma vulnerabilidad.

En marzo de 2017, Microsoft emitió el boletín de seguridad MS17-010 en el que se detallaba el fallo de seguridad EternalBlue y anunció parches para Windows para todas las versiones compatibles activas en ese momento, incluyendo Windows Vista, Windows 7, 8.1 y 10, Windows Server 2008, 2012 y 2016. EternalBlue también está cubierto por CVE-2017-0143 a CVE-2017-0148.

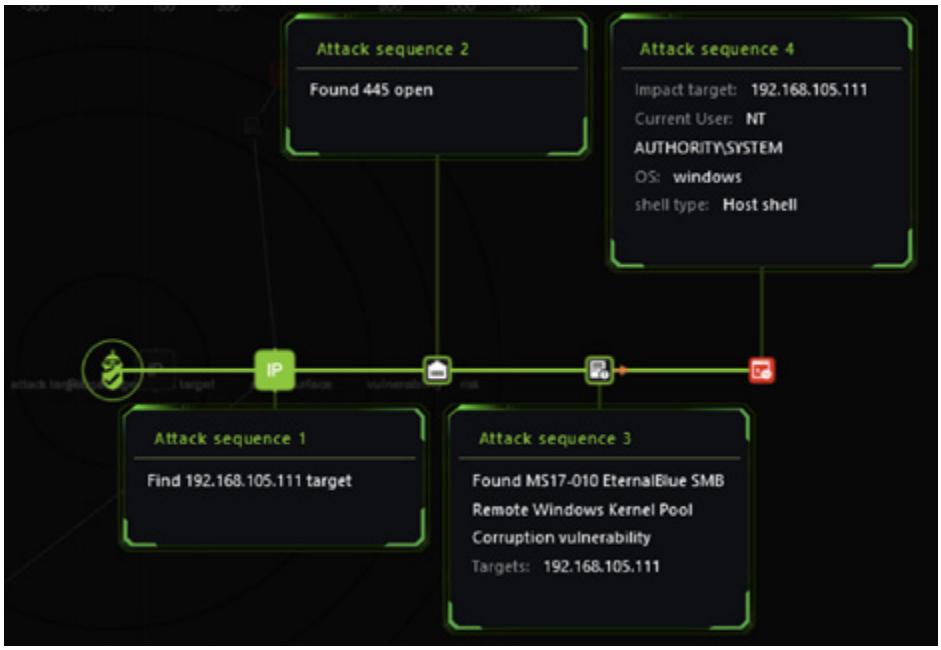
EternalBlue es un exploit que permite a los actores de amenazas obtener acceso a un activo de Windows, controlar el shell y ejecutar remotamente código arbitrario mediante el envío de paquetes especialmente diseñados a un servidor que utiliza Microsoft Server Message Block 1.0 (SMBv1). SMB es un protocolo de compartición de archivos en red que permite acceder a los archivos de un servidor remoto.

Esta vulnerabilidad permite a los actores de la amenaza inyectar malware que luego se autopropaga para infectar toda la red y todos los dispositivos conectados a ella, dejando caer la carga útil del cripto-ransomware por todas partes a medida que se propaga. La capacidad de autopropagación ha convertido a EternalBlue en un exploit popular para otros programas maliciosos como Trickbot (un troyano bancario modular), así como CoinMiner y WannaMine, donde los mineros de criptomonedas explotan EternalBlue para obtener acceso a los recursos informáticos para minar criptomonedas.

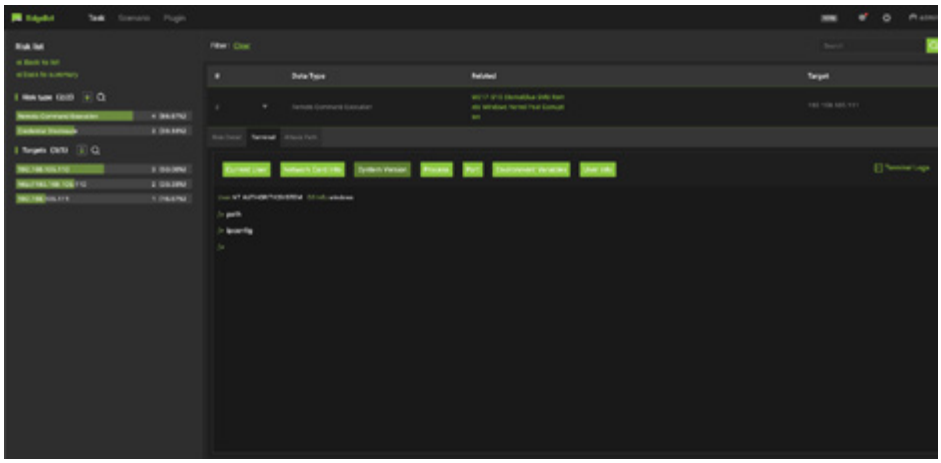
A pesar de que la vulnerabilidad EternalBlue -y los parches de Windows para contrarrestarla- ya se anunciaron hace años, en marzo de 2017, todavía hay suficientes máquinas sin parchear a principios de 2021 para que este exploit sea muy atractivo para los actores de amenazas.

RidgeBot 3.2 puede escanear su red, dispositivos y servidores para detectar cualquier vulnerabilidad latente sin parche de EternalBlue en su entorno. RidgeBot lanza además un ataque contra el dispositivo objetivo explotando la vulnerabilidad EternalBule encontrada. En el ejemplo de ataque de Ridgebot contra la IP 192.168.105.111 que se muestra a continuación, se logró penetrar una vulnerabilidad EternalBlue (recuadro rojo en el borde exterior).

Al profundizar en la ruta de explotación (cuadros verdes) hasta la máquina objetivo comprometida (cuadro rojo), se revela la ruta de ataque que el actor de la amenaza explotó para llegar al objetivo.



Para los exploits de EternalBlue, RidgeBot puede controlar el shell del host del dispositivo comprometido. Un exploit RidgeBot exitoso de una vulnerabilidad EternalBlue se da en la Tabla de Riesgos, mostrando que el objetivo del host fue ingresado y que RidgeBot pudo emitir comandos desde el shell.



Ejecución remota de código/comando: Struts2

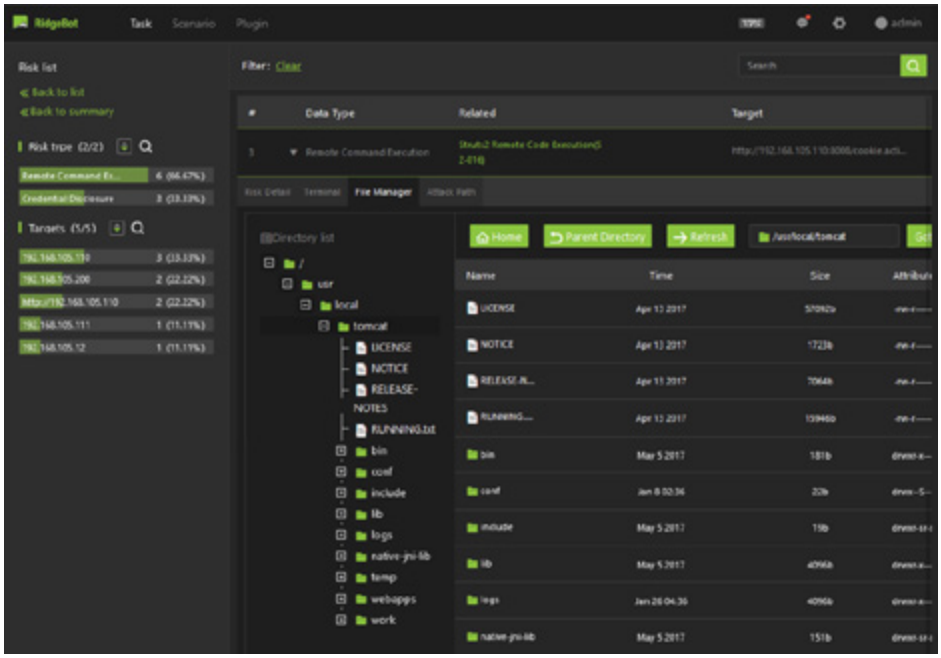
Apache Struts2 es un marco de trabajo de aplicaciones web (Modelo-Vista-Controlador, o MVC) gratuito y de código abierto para desarrollar aplicaciones web Java multiplataforma. Tiene una arquitectura extensible que utiliza la API de Java Servlet y plugins REST, AJAX y JSON para facilitar el desarrollo de software.

Existe una serie de vulnerabilidades de ejecución remota de código en el código y los plugins de Struts2, incluyendo los boletines de seguridad de Apache S2-008 (CVE-2012-0391), S2-016, S2-019 (CVE-2013-4316), S2-032, S2-037, S2-045, S2-048, S2-052, S2-057 y S2-059. Puede revisar los detalles de todos los boletines de seguridad de Apache Struts2 aquí.

RidgeBot 3.2 puede escanear su red, dispositivos y servidores para detectar cualquiera de las vulnerabilidades de Struts2 mencionadas anteriormente en su entorno. Además, RidgeBot lanza un ataque contra el dispositivo objetivo explotando la vulnerabilidad Struts2 encontrada. En el ejemplo de ataque de Ridgebot contra la IP 192.168.105.110 que se muestra a continuación, se logró penetrar una vulnerabilidad de Struts2 (cuadro rojo en el borde exterior).

Al profundizar en la ruta de explotación (cuadros verdes) hasta la máquina objetivo comprometida (cuadro rojo), se revela la ruta de ataque que el actor de la amenaza explotó para llegar al objetivo.

Para los exploits de Struts2, RidgeBot puede cosechar el directorio de archivos del host objetivo. Un exploit RidgeBot exitoso de una vulnerabilidad Struts2 se da en la Tabla de Riesgos, mostrando que el host objetivo fue ingresado y su directorio de archivos es visible para RidgeBot.



Ataques de divulgación de credenciales/contraseñas débiles

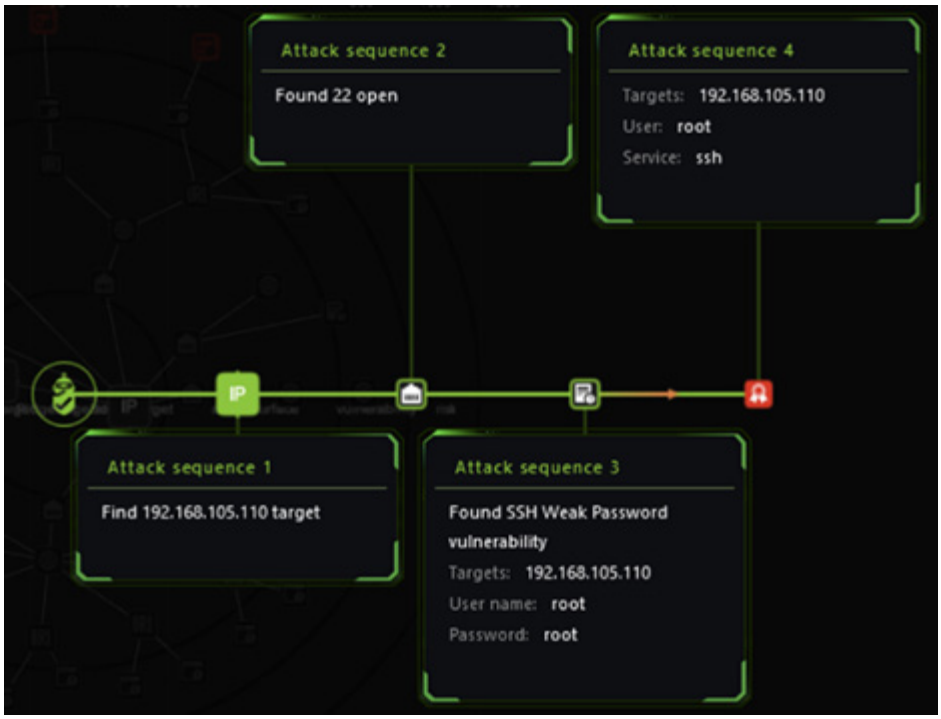
Existen numerosas vulnerabilidades conocidas relacionadas con las contraseñas débiles, o la divulgación de credenciales, en la industria, incluyendo las asociadas a SSH, Redis, SQL Server, SMB y Microsoft Remote Desktop Server. Algunos de los exploits están relacionados con la divulgación de credenciales, otros con RCE abriendo oportunidades “wormables” donde el malware puede propagarse de un ordenador vulnerable a otro, de manera similar a como se propagó el ransomware WannaCry.

RidgeBot 3.2 puede escanear su red, dispositivos y servidores para detectar una sección transversal de vulnerabilidades de contraseñas débiles en su entorno. Además, RidgeBot lanza un ataque contra el dispositivo objetivo explotando la vulnerabilidad de la contraseña débil encontrada. En el ejemplo de ataque de Ridgebot contra la IP 192.168.105.110 que se muestra a continuación, se logró penetrar una vulnerabilidad de contraseña débil de Redis (cuadro rojo en el borde exterior).

Al profundizar en la ruta de explotación (cuadros verdes) hasta la máquina objetivo comprometida (cuadro rojo), se revela la ruta de ataque que el actor de la amenaza explotó para llegar al objetivo.

En un ejemplo de escaneo y ataque de Ridgebot contra la IP 192.168.105.110 que se muestra a continuación, se penetró una vulnerabilidad de contraseña débil de SSH (cuadro rojo en el borde exterior).

Al profundizar en la ruta de explotación (cuadros verdes) hasta la máquina objetivo comprometida (cuadro rojo), se revela la ruta de ataque que el actor de la amenaza explotó para llegar al objetivo.



WebLogic y otros ataques de carga de archivos

Las vulnerabilidades de carga de archivos utilizan archivos para insertar código malicioso que desencadena RCE en la plataforma de destino.

- **Vulnerabilidad de carga de archivos local:** Una aplicación permite a un actor de la amenaza cargar directamente un archivo malicioso, que posteriormente se ejecuta.
- **Vulnerabilidad de carga de archivos remota:** Una aplicación aprovecha la acción del usuario para obtener un archivo de un sitio remoto en Internet y almacenarlo localmente para ser ejecutado en un momento posterior.

RidgeBot 3.2 puede escanear su red, dispositivos y servidores para detectar las siguientes vulnerabilidades de carga de archivos en su entorno.

- El método PUT de Apache Tomcat escribe archivos (CVE-2017-12615)
- La página de configuración de prueba del servicio WebLogic tiene una carga arbitraria de archivos (CVE-2018-2894)
- Deserialización del decodificador XML de WebLogic (CVE-2017-10271)
- Escritura arbitraria de archivos en Apache ActiveMQ (CVE-2016-3088)

Implantación de RidgeBot 3.2 Ridge Security Demo

Una vez que un individuo que representa una amenaza se ha infiltrado en su red y ha progresado hasta establecer un punto de apoyo dentro de sus activos, a menudo es demasiado tarde para detener el daño. Por lo tanto, es imperativo evitar que los actores de amenazas comprometan sus activos, impidiéndoles encontrar cualquier abertura por la que puedan entrar en su red y en sus activos.

RidgeBot 3.2 contiene capacidades críticas de exploración y explotación desarrolladas específicamente para combatir las vulnerabilidades que conducen a los ataques de ransomware dirigidos. Póngase en contacto con nosotros hoy mismo para obtener una demostración de cómo RidgeBot puede ayudar a su organización a sobrevivir en estos tiempos peligrosos.

Company Profile

Ridge Security delivers ethical, efficient and affordable pen testing solutions to enterprises, small and large. We ensure our customers stay compliant, alerted and secure at all times in the cyber world. The management team has many years of networking and security experience. Ridge Security is located in the heart of Silicon Valley and is expanding into other areas including Latin America, Asia and Europe.

RidgeBot, a robotic penetration testing system, fully automates the testing process by coupling ethical hacking techniques to decision-making algorithms. RidgeBots locate, exploit and document business risks and vulnerabilities discovered during the testing process, highlighting the potential impact or damage.

Ridge Security Technology Inc.
www.ridgesecurity.ai