5 señales de que tu organización será víctima de ransomware

Por Peter Mackenzie, Global Malware Escalations Manager de Sophos

Cuando en Sophos trabajamos con víctimas de ransomware, hacemos una revisión a las últimas dos semanas previas a la detección del ataque. En ese periodo de tiempo es común encontrar algunos indicadores que nos hacen saber de inmediato en dónde fue vulnerado el sistema afectado. Cualquiera de los indicadores que enlistamos a continuación son una señal de que los atacantes ya tenían una idea de cómo es la red afectada y cómo podrían obtener las cuentas y los accesos necesarios para lanzar sus ataques.

Actualmente, los atacantes utilizan herramientas de administración legítimas para preparar el escenario para lanzar sus ataques. Estas cinco señales pueden pasar por alto fácilmente o ser difíciles de detectar por el personal de TI de una empresa, pero son indicadores muy claros de que se avecina un ransomware:

1. Escáneres de red, especialmente en un servidor

Los atacantes generalmente comienzan por obtener acceso a una máquina donde buscan información básica; es una Mac o Windows, cuál es el dominio y el nombre de la empresa, qué tipo de derechos de administrador tiene la computadora y más. Luego, los atacantes querrán saber qué más hay en la red y a que pueden acceder. La forma más fácil de determinar esto es escanear la red. Si se detecta un escáner de red, como AngryIP o Advanced Port Scanner, se debe acudir de inmediato al personal de TI para saber si este escáner fue instalado por ellos. Si nadie resulta responsable, es hora de investigar.

2. Herramientas para deshabilitar el software antivirus

Una vez que los atacantes tienen derechos de administrador, a menudo intentarán deshabilitar el software de seguridad utilizando aplicaciones creadas para la eliminación forzada de software, como Process Hacker, IOBit Uninstaller, GMER y PC Hunter. Este tipo de herramientas comerciales son legítimas, pero en las manos equivocadas son muy peligrosas. Si al detectarse que no hay algún software que requiera ser eliminado, entonces el personal de ciberseguridad debe encender las alertas y preguntarse seriamente por qué aparecieron de repente.

3. Presencia de MimiKatz

Primero entendamos qué es MimiKatz: se trata de una aplicación de código abierto que permite robar datos de identificación y credenciales de usuarios de una red para brindar acceso de forma ilegal a los sistemas y explotar vulnerabilidades del mismo. Esta herramienta fue creada para detectar vulnerabilidades en Windows, y es muy usada por atacantes actualmente.

Cualquier detección de esta aplicación debe ser de inmediato investigada. Los atacantes también suelen usan Microsoft Process Explorer, incluido en Windows Sysinternals, que es una herramienta legítima que se infiltra en los equipos creando un archivo en formato .dmp. Una vez dentro, instalan MimiKatz para extraer de forma segura los nombres de usuario y las contraseñas.

4. Patrones de comportamiento sospechoso

El personal de TI debe estar atento a cualquier patrón de comportamiento que ocurra a la misma hora todos los días, o de forma repetitiva, ya que esto es a menudo una indicación de que algo sospechoso sucede, incluso si se han detectado y eliminado archivos maliciosos.

5. Ataques de 'prueba'

Ocasionalmente, los atacantes implementan pequeños ataques de prueba en algunas computadoras para ver si el método de implementación y el ransomware se ejecuta con éxito, o si el software de seguridad lo detiene. Si las herramientas de seguridad detienen el ataque, cambian sus tácticas e intentan nuevamente. Esto les ayudará a saber qué tan limitado es su tiempo de ataque y que tan fuertes son las medidas de seguridad implementadas en el objetivo. A menudo es cuestión de horas antes de que se lance un ataque mucho más grande, por lo que ante un ataque de este tipo la acción debe ser inmediata.

Las empresas en la actualidad deben estar atentas al ransomware ya que se trata de algo más común de lo que parece. De acuerdo con el estudio *El estado del ransomware 2020* de Sophos, el 51% de las organizaciones a nivel global fueron víctimas de este tipo de 'secuestros de datos' durante 2019, lo cual representa pérdidas de hasta 1.4 millones de dólares para las empresas.

###

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos,

phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X y el Firewall XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido. Para obtener más información visita www.sophos.com

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/