Sophos descubre una nueva versión del ransomware *Snatch*

Un informe detalla los cambios en las TTPs de Snatch, incluyendo el reinicio del PC en modo seguro.

Ciudad de México a 17 de diciembre de 2019. – Sophos (LSE: SOPH), líder global en ciberseguridad de última generación, ha presentado un informe relacionado con su investigación: Snatch, el ransomware que reinicia la PC en modo seguro para evitar los protocolos de seguridad, elaborado por SophosLab y el Sophos Managed Threat Response. Dicho estudio detalla los cambios en el método de ataque de *Snatch* –identificado por primera vez en diciembre del 2018– los cuales ahora incluyen el reinicio de PCs en modo seguro durante el ataque para evadir las conductas de protección que detectan la actividad de ransomware. Sophos considera que se trata de una nueva técnica adoptada por ciberdelincuentes para evadir los protocolos de seguridad.

Como indica la tendencia señalada en el Informe sobre Ciberamenazas 2020 de Sophos, los ciberdelincuentes de *Snatch* podrían estar extrayendo datos incluso antes del ataque del ransomware. Este comportamiento ha sido utilizado por otros grupos criminales como Bitpaymer. Sophos prevé que esta secuencia de extracción previa a la encriptación continúe.

Este ransomware es un claro ejemplo de un ataque activo y automatizado. Una vez que los atacantes logran ingresar gracias al abuso en los servicios de acceso remoto, usan el teclado manualmente para burlar la seguridad y efectuar el daño. Como lo explica el informe Snatch, los atacantes están entrando a través de los servicios de acceso remoto inseguros de TI, tales como el Protocolo de Escritorio Remoto (RDP). El informe también muestra ejemplos del reclutamiento de criminales experimentados para comprometer los servicios de acceso remoto a través de foros en la *dark web*.

Consejos para los defensores

- Ser proactivo en la búsqueda de amenazas: utilice un equipo interno o externo experto en operaciones de seguridad para monitorear amenazas las 24 horas del día.
- Habilite *machine/deep* learning, mitigaciones de adversarios y detección de comportamientos en la seguridad de puntos finales.
- Siempre que sea posible, identifique y apague los servicios de acceso remoto expuestos a la red pública.
- Si requiere de acceso remoto, utilice una VPN con las mejores prácticas del sector como la autenticación multifactorial, auditorías de contraseñas y control de acceso preciso, además de supervisar activamente el acceso remoto.
- Cada servidor con acceso remoto abierto a la red pública necesitará los parches actualizados, ser protegida mediante controles preventivos (como software que

proteja los puntos finales) y monitorear activamente anomalías de acceso y otros comportamientos poco comunes.
- Los usuarios registrados en los servicios de acceso remoto deberán tener privilegios limitados para el resto de la red corporativa.
- Los administradores deberán adoptar autenticación multifactorial y usar una cuenta administrativa aparte de su cuenta de usuario normal.
- Monitoreo activo de puertos RDP abiertos en el espacio del IP público.

Para mayor información y detalles técnicos precisos acerca del ransomware *Snatch*, por favor consulte SophosLabs Uncut.

# # #

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, **Sophos** protege a casi 400 mil organizaciones de todos los tamaños en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrollado por SophosLabs -un equipo global de *Threat Intelligence* y *Data Science*- las soluciones nativas de la nube y mejoradas por IA de Sophos, aseguran protección en puntos finales (computadoras portátiles, servidores y dispositivos móviles) y redes contra tácticas y técnicas cibercriminales en evolución, incluidas las filtraciones de adversarios activos y automáticos, ransomware, malware, exploits, exfiltración de datos, phishing y más. La galardonada plataforma basada en la nube de Sophos Central integra toda la cartera de productos de **Sophos**, desde la solución de punto final, Intercept X, hasta el Firewall XG, en un único sistema llamado Seguridad Sincronizada. Los productos de **Sophos** están disponibles exclusivamente a través de un canal global de más de 47 mil socios y proveedores de servicios gestionados (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, y cotiza en la Bolsa de Londres bajo el símbolo "SOPH". Más información está disponible en www.sophos.com

Síguenos en:

Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/Sophos
LinkedIn: https://www.linkedin.com/company/sophos/
Instagram: https://www.instagram.com/sophossecurity/?hl=es-la
Youtube: https://www.youtube.com/user/SophosProducts

Contacto

Fernanda Cornejo
fernando.cornejo@another.co

Mario García
mario@another.co
M.: 55 3930 2474