Entropy: el ransomware que ‘adoptó’ el código de la botnet Dridex

CIUDAD DE MÉXICO. 23 de febrero de 2022.- Sophos, líder mundial en ciberseguridad de última generación, lanzó el estudio "Dridex Bots Deliver Entropy in Recent Attacks", que detalla las similitudes de código en la botnet Dridex y el ransomware conocido, Entropy.

Las similitudes se encuentran en el paquete de software utilizado para ocultar el código de ransomware, en las subrutinas de malware diseñadas para encontrar y ofuscar comandos (API) y en los procesos utilizados para descifrar texto encriptado.

Sophos descubrió las similitudes mientras investigaba dos incidentes en los que los atacantes usaron Dridex para lanzar el ransomware Entropy. Estos ataques se dirigieron a una empresa del sector de medios de comunicación y una agencia gubernamental, utilizando versiones personalizadas en algunas de las computadoras de los objetivos.

Los atacantes extrajeron datos a proveedores de almacenamiento en la nube utilizando la herramienta de compresión legítima WinRAR, antes de lanzar el ransomware en equipos desprotegidos.

“No es raro que los operadores de malware compartan, tomen prestado o roben el código de otros, ya sea para ahorrarse el esfuerzo de crear su propia atribución, engañar intencionalmente o distraer a los investigadores de seguridad. Este enfoque hace que sea más difícil encontrar evidencia que corrobore una 'familia' de malware relacionado o identificar 'señales falsas' que pueden facilitar el trabajo de los atacantes y dificultar el trabajo de los investigadores”, dijo Andrew Brandt, investigador principal de Sophos.

“En este análisis, Sophos se centró en aspectos del código que aparentemente tanto Dridex como Entropy usaban para hacer que el análisis fuera más desafiante. Estos incluyen el código de empaquetado, que evita el análisis estático fácil del malware subyacente, una rutina que los programas usan para ocultar las llamadas de comando (API) que realizan y que descifra las cadenas de texto cifradas incrustadas en el malware. Los investigadores descubrieron que esos procesos, en ambos programas maliciosos, tienen un flujo de código y una lógica fundamentalmente similares”, explica.

- **Mismo código, metodología de ataque diferente**

Además de encontrar similitudes en el código, los investigadores de Sophos encontraron que en el ataque a la organización de medios, los adversarios utilizaron el exploit ProxyShell para apuntar a un servidor vulnerable para instalar un código malicioso, que luego aprovecharon para difundir balizas Cobalt Strike a otras computadoras. Los atacantes estuvieron en la red durante cuatro meses antes de lanzar Entropy a principios de diciembre de 2021.

En el ataque a la organización del gobierno regional, el objetivo fue infectado con el malware Dridex a través de un archivo adjunto de correo electrónico malicioso. Luego, los atacantes usaron Dridex para propagar malware adicional y moverse lateralmente dentro de la red del objetivo. El análisis de incidentes muestra que aproximadamente 75 horas después de la detección inicial de un intento de inicio de sesión sospechoso en una máquina, los atacantes comenzaron a robar datos y trasladarlos a una serie de proveedores de nube.

- **¿Cómo protegerse?**

La investigación encontró que en ambos casos, los atacantes pudieron aprovechar sistemas Windows vulnerables y sin parches para abusar de herramientas legítimas. La aplicación periódica de parches de seguridad y la investigación activa de alertas sospechosas por parte de los cazadores de amenazas y los equipos de operaciones de seguridad ayudarán a dificultar que los atacantes obtengan acceso inicial a un objetivo e implementen código malicioso.

###

Sobre Sophos

Sophos es un líder mundial en ciberseguridad de próxima generación y protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología de inteligencia de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de gestión integrada basada en la nube, Sophos Central, la pieza central de un ecosistema de ciberseguridad adaptable que cuenta con un lago de datos centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay más información disponible en www.sophos.com

Síguenos en:

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