ESET revela una investigación sobre ataques a sitios web en Medio Oriente vinculado al software espía Candiru

El equipo de investigación de ESET identificó una campaña de compromiso de sitios web estratégicos (watering hole) contra sitios web de alto perfil en el Medio Oriente, con un fuerte enfoque en Yemen. Los ataques están vinculados a Candiru, una empresa que vende herramientas de software ofensivas de última generación y servicios relacionados a agencias gubernamentales. Los sitios web victimizados pertenecen a medios de comunicación en el Reino Unido, Yemen y Arabia Saudita, así como a Hezbollah; a instituciones gubernamentales en Irán (Ministerio de Relaciones Exteriores), Siria (incluido el Ministerio de Electricidad) y Yemen (incluidos los Ministerios del Interior y Finanzas); a los proveedores de servicios de Internet en Yemen y Siria; ya empresas de tecnología aeroespacial/militar en Italia y Sudáfrica. Los atacantes también crearon un sitio web que imitaba una feria médica en Alemania.

Un ataque de este estilo se basa en comprometer los sitios web que probablemente sean visitados por objetivos de interés, lo que abre la puerta a infectar la máquina de un visitante del sitio web. En esta campaña, los visitantes específicos de estos sitios web probablemente fueron atacados a través de un exploit del navegador. Sin embargo, los investigadores de ESET no pudieron conseguir un exploit o el payload final. Esto muestra que los actores de las amenazas han optado por limitar el enfoque de sus operaciones y no quieren utilizar -y consecuentemente revelar- sus exploits zero-day, lo que demuestra cuán altamente dirigida es esta campaña. Los sitios web comprometidos solo se utilizan como punto de partida para alcanzar los objetivos finales.

“En 2018, desarrollamos un sistema interno personalizado para descubrir ataques de watering hole (también conocidos como compromiso de sitios web estratégicos) en sitios web de alto perfil. El 11 de julio de 2020, nuestro sistema nos notificó que el sitio web de la embajada iraní en Abu Dhabi estaba contaminado con código JavaScript malicioso. Nuestra curiosidad se despertó por la naturaleza de alto perfil del sitio web objetivo, y en las siguientes semanas notamos que otros sitios web con conexiones a Oriente Medio también fueron objetivo ”, dice el investigador de ESET **Matthieu Faou**, quien descubrió las campañas.

“El grupo de amenazas se mantuvo en silencio hasta enero de 2021, cuando observamos una nueva ola de compromisos. Esta segunda ola duró hasta agosto de 2021, cuando todos los sitios web fueron limpiados nuevamente como fue el caso en 2020, probablemente por los propios perpetradores”, agrega.

“Los atacantes también imitaron un sitio web perteneciente a la feria comercial MEDICA del Foro Mundial de Medicina celebrada en Düsseldorf, Alemania. Los operadores clonaron el sitio web original y agregaron un pequeño fragmento de código JavaScript. Es probable que los atacantes no pudieran comprometer el sitio web legítimo y tuvieran que configurar uno falso para inyectar su código malicioso”, dice Faou.

Durante la campaña de 2020, el malware verificó el sistema operativo y el navegador web. La amenaza continuaba con sus funcionalidades solo si el equipo contaba con un sistema operativo Windows o macOS, lo que sugiere que la campaña no estaba dirigida a dispositivos móviles. En la segunda ola, para ser un poco más sigilosos, los atacantes comenzaron a modificar los scripts que ya estaban en los sitios web comprometidos.

“En una entrada de blog sobre Candiru de Citizen Lab en la Universidad de Toronto, la sección llamada ‘¿Un clúster vinculado a Arabia Saudita?’ Menciona un documento de spearphishing que se cargó en VirusTotal y en varios dominios operados por los atacantes. Los nombres de dominio son variaciones de acortadores de URL genuinos y sitios web de análisis web, que es la misma técnica utilizada para los dominios que se ven en los ataques de watering holes”, explica Faou, vinculando los ataques a Candiru.

Por lo tanto, existe una probabilidad significativa de que los operadores de las campañas sean clientes de Candiru. Los creadores de los documentos y los operadores de los watering hole potencialmente también sean los mismos. Candiru es una empresa israelí privada de software espía que se agregó recientemente a la lista de entidades del Departamento de Comercio de EE. UU. Esto puede impedir que cualquier organización con sede en EE.UU. Haga negocios con Candiru sin obtener primero una licencia del Departamento de Comercio.

ESET dejó de ver la actividad de esta operación a fines de julio de 2021, poco después del lanzamiento de publicaciones de blog por parte de Citizen Lab, Google y Microsoft que detallaban las actividades de Candiru.