I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Loader

Nivel de riesgo: Medio

II. ALERTA

Actores maliciosos estarían utilizando a los archivos de instalación de aplicaciones populares como Zoom, Cisco AnyConnect, ChatGPR, etc., para distribuir el malware Bumblebee.

Figura 1.- Ilustración relacionada al malware Bumblebee
Fuente: Elaboración Propia

III. INTRODUCCIÓN

Los programas maliciosos “loaders” cumplen funciones asistenciales para subsiguientes etapas en la infección de sistemas de información con programas maliciosos malware. Los loaders cuentan con varios módulos para ejecución de payload, ya sea de manera remota o localmente con código existente en el mismo loader.

Recientemente se han ejecutado varias campañas de ataques de tipo ransomware, que dependen de las capacidades específicas de los programas maliciosos loader, como son el caso de Conti y Diavol. Las campañas de ataque de estos grupos se han caracterizado por ejecutar los payloads de Cobalt Strike, que a su vez representan un alto riesgo de comprometimiento de sistemas de información.

El análisis de comportamiento del malware Bumblebee indica la instalación de varios tipos de malware tanto para el comprometimiento del sistema en el cual se descargó así como para propagarse hacia otros sistemas. Adicionalmente en lo que respecta a la actualización del malware Bumblebee se ha detectado la herramienta PowerSploit a fin de inyectar archivos DLL en la memoria del sistema

IV. VECTOR DE ATAQUE:

- Elementos de publicidad en plataformas confiables como Google Ads
- Correos electrónicos provenientes de nombres de dominio que parecen legítimos.

V. IMPACTO:

- Administración remota no autorizada del sistema.
- Filtración de activos de información.
- Comprometimiento de credenciales de acceso y sistemas de información.

VI. INDICADORES DE COMPROMISO

Tipo	Dato
Domain Name	appcisco.com
Domain Name	baveyek.com
MD5	e4a5383ac32d5642eaf2c7406a0f1c0f

Tipo	Dato
MD5	522c0b0d445c62cdeb0a80bcce645d57
MD5	6f7e07b84897cccab30594305416d36f
MD5	711482ca4d5dcaf0aec4c7c4b3e1bef1
Dirección IP	173.44.141.131
Dirección IP	172.93.193.3:443
Dirección IP	23.81.246.22:443
Dirección IP	95.168.191.134:443
Dirección IP	104.168.175.78:443
Dirección IP	172.93.193.46:443
Dirección IP	157.254.194.104:443

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Instalar y mantener actualizado un programa antivirus.
- No abrir y ejecutar los enlaces y archivos adjuntos en correos electrónicos de fuentes desconocidas.
- No descargar programas y aplicaciones desde lugares diferentes a los sitios propios de los desarrolladores.

VIII. REFERENCIAS:

- Secureworks. Bumblebee Malware Distributed via trojanized installer download. (20 de 05 de 2022). Obtenido de https://www.packetlabs.net/posts/bumblebee-malware/.
- Packetlabs. What us Bumblebee malware. (16 de 05 de 2022). Obtenido de https://www.packetlabs.net/posts/bumblebee-malware/.