Trellix muestra el modus operandi de Scattered Spider

Por Phelix Oluoch*

Scattered Spider, también conocido como UNC3944, Scatter Swine, Muddled Libra y Roasted 0ktapus, es un grupo de actores de amenazas motivado financieramente que ha estado activo desde mayo de 2022. Scattered Spider se ha observado en gran medida apuntando a organizaciones de telecomunicaciones y subcontratación de procesos comerciales (BPO). Sin embargo, la actividad reciente indica que este grupo ha comenzado a apuntar a otros sectores, incluidas las organizaciones de infraestructura crítica.

A pesar de este cambio en los objetivos, Scattered Spider continúa aprovechando una variedad de tácticas de ingeniería social, incluido el phishing de Telegram y SMS, el intercambio de SIM, la fatiga de MFA y otras tácticas como parte de sus ataques. A menudo se ha observado que este grupo se hace pasar por personal de TI para convencer a las personas de que compartan sus credenciales o concedan acceso remoto a sus computadoras, se ha relacionado con varias campañas de phishing anteriores e implementaciones de controladores de kernel maliciosos, incluido el uso de una versión firmada pero maliciosa de Windows. Controlador de diagnóstico Intel Ethernet.

Este artículo profundiza en el modus operandi de Scattered Spider; los eventos recientes y las herramientas aprovechadas por el actor de amenazas, las vulnerabilidades explotadas y su impacto.

Eventos recientes

Scattered Spider generalmente explota vulnerabilidades como CVE-2015-2291 y utiliza herramientas como STONESTOP y POORTRY para finalizar el software de seguridad y evadir la detección. El grupo demuestra un conocimiento profundo del entorno de Azure y aprovecha las herramientas integradas para sus ataques. Una vez obtenido el acceso inicial, se ha observado a Scattered Spider realizando un reconocimiento de varios entornos, incluidos Windows, Linux, Google Workspace, Azure Active Directory, Microsoft 365 y AWS, además de realizar movimientos laterales y descargar herramientas adicionales para filtrar VPN y Datos de inscripción de MFA en casos seleccionados. También se sabe que el grupo establece persistencia a través de herramientas legítimas de acceso remoto como AnyDesk, LogMeIn y ConnectWise Control.

Para enero de 2023, Scattered Spider estuvo involucrada en más de media docena de incidentes desde mediados de 2022 hasta principios de 2023 en los que se dirigieron a grandes empresas de subcontratación que prestan servicios a instituciones e individuos de criptomonedas de alto valor.

En diciembre de 2022, Scattered Spider realizó campañas dirigidas a organizaciones de telecomunicaciones y BPO. El objetivo de la campaña parecía ser obtener acceso a las redes de los operadores móviles y, como se evidencia en dos investigaciones, realizar actividades de intercambio de SIM. El acceso inicial fue variado: ingeniería social usando llamadas telefónicas y mensajes de texto para hacerse pasar por personal de TI, y ya sea dirigiendo a las víctimas a un sitio de recolección de credenciales o dirigiendo a las víctimas para que ejecuten herramientas comerciales de administración y monitoreo remoto (RMM). Las campañas fueron

extremadamente persistentes y descaradas. Una vez que se contuvo al adversario o se interrumpieron las operaciones, inmediatamente se movieron para apuntar a otras organizaciones dentro de los sectores de telecomunicaciones y BPO.

En el mismo mes, se descubrió su uso de una firma de atestación para firmar malware. Microsoft reveló los pasos que tomó para implementar protecciones de bloqueo y suspender las cuentas que se usaron para publicar controladores maliciosos que fueron certificados por su Programa de desarrollo de hardware de Windows. El problema se inició después de que se notificara a Microsoft sobre el uso de controladores no autorizados en los esfuerzos posteriores a la explotación, incluida la implementación de ransomware.

En agosto de 2022, Twilio identificó acceso no autorizado a la información relacionada con 163 clientes, incluido Okta. Los números de teléfono móvil y los mensajes SMS asociados que contenían contraseñas de un solo uso eran accesibles para Scattered Spider a través de la consola de Twilio. El kit de phishing utilizado por el actor de amenazas fue diseñado para capturar nombres de usuario, contraseñas y factores OTP y empresas de tecnología, proveedores de telecomunicaciones y organizaciones e individuos vinculados a la criptomoneda.

Herramientas

Scattered Spider usa POORTRY y STONESTOP para finalizar el software de seguridad y evadir la detección.

POORTRY es un controlador malicioso que se utiliza para finalizar procesos seleccionados en sistemas Windows, por ejemplo, el agente de detección y respuesta de punto final (EDR) en un punto final. Para evadir la detección, los atacantes firmaron el controlador POORTRY con una firma de Authenticode de compatibilidad de hardware de Microsoft Windows.

STONESTOP es una utilidad de usuario de Windows que intenta terminar procesos creando y cargando un controlador malicioso. Funciona como un cargador/instalador para POORTRY, así como un orquestador para instruir al conductor sobre qué acciones realizar.

En abril de 2023, el grupo de ransomware ALPHV (BlackCat) usó una versión actualizada de POORTRY para comprometer al gigante estadounidense de pagos NCR, lo que provocó una interrupción en su plataforma de punto de venta Aloha.

Explotación de vulnerabilidades

Se sabe que Scattered Spider explota CVE-2015-2291, que es una vulnerabilidad en el controlador de diagnóstico Intel Ethernet para Windows (iqvw64.sys) que permite a los usuarios locales provocar una denegación de servicio o posiblemente ejecutar código arbitrario con privilegios de kernel a través de un (a) 0x80862013, (b) 0x8086200B, (c) 0x8086200F o (d) 0x80862007 llamada IOCTL. Scattered Spider aprovechó CVE-2015-2291 para implementar un controlador de kernel malicioso en el controlador de diagnóstico Intel Ethernet para Windows (iqvw64.sys).

Además, Scattered Spider ha explotado CVE-2021-35464, que es una falla en el servidor ForgeRock AM. Las versiones del servidor ForgeRock AM anteriores a la 7.0 tienen una vulnerabilidad de deserialización de Java en el parámetro jato.pageSession en varias páginas. La explotación no requiere autenticación, y la ejecución remota de código se puede activar enviando una sola solicitud /ccversion/* diseñada al servidor. La vulnerabilidad existe debido al

uso de Sun ONE Application Framework (JATO) que se encuentra en versiones de Java 8 o anteriores. Scattered Spider explotó CVE-2021-35464 para ejecutar código y elevar sus privilegios sobre el usuario de Apache Tomcat en una instancia de AWS. Esto se logró solicitando y asumiendo los permisos de un rol de instancia utilizando un token de AWS comprometido.

Impacto

Scattered Spider es conocido por el robo de datos confidenciales y el aprovechamiento de la infraestructura organizacional confiable para ataques de seguimiento en clientes intermedios.

Cobertura de productos Trellix

Los sistemas de seguridad de Trellix para Endpoint, Red y correos electrónicos, ofrecen una estrategia de detección de varias capas para las actividades de Scattered Spider, que incluye comprobaciones de los IOC y análisis de comportamiento para garantizar que se descubra cualquier amenaza potencial y se evite que perjudique a nuestros clientes. Para adelantarse a las amenazas nuevas y en evolución, nuestros productos monitorean y actualizan continuamente sus bases de datos de inteligencia de amenazas. Eso incluye Trellix Multi-Vector Virtual Execution Engine, un nuevo motor central antimalware, clasificación de comportamiento de aprendizaje automático y motores de correlación de IA, inteligencia de amenazas en tiempo real de Trellix Dynamic Threat Intelligence (DTI) Cloud y defensas en todo el Ataque el ciclo de vida para mantener su organización más segura y resistente.

---

* Phelix Oluoch es un investigador de ciber amenazas de Trellix con dieciséis años de experiencia en seguridad de la información, así como habilidades y conocimientos de adaptación para ejecutar y respaldar operaciones de seguridad. Tiene experiencia técnica y de gestión en las industrias farmacéutica, de salud, de petróleo y gas, financiera y de transporte; así como en la remediación de incidentes APT. Certificaciones CISM, CISSP, CDPSE, (ISC)² CCSP, GCIA y GCFE y tiene una Maestría en Ciencias en Tecnologías de Seguridad de la Universidad de Minnesota. Entrena, educa y asesora a los Marines estadounidenses a través del programa Cyber Auxiliary del US Marine Corps. También es mentor de ISACA.