Una nueva campaña de malware está aprovechando una vulnerabilidad en el sistema de invitaciones de Discord para distribuir un ladrón de información llamado Skuld y el troyano de acceso remoto AsyncRAT.

> *"Los atacantes secuestraron los enlaces mediante el registro de enlaces personalizados (vanity links), lo que les permitió redirigir silenciosamente a los usuarios desde fuentes confiables hacia servidores maliciosos. Combinando la técnica de phishing ClickFix, cargadores por etapas y evasión basada en tiempo, lograron entregar de forma sigilosa el AsyncRAT junto con una versión personalizada de Skuld Stealer, dirigida a monederos de criptomonedas»*, señaló Check Point en un informe técnico.

El problema con el mecanismo de invitaciones de Discord radica en que permite a los atacantes tomar control de enlaces de invitación caducados o eliminados y redirigir a los usuarios desprevenidos a servidores controlados por los atacantes. Esto implica que un enlace de invitación que antes era legítimo y compartido en foros o redes sociales puede, sin saberlo, dirigir a los usuarios hacia sitios maliciosos.

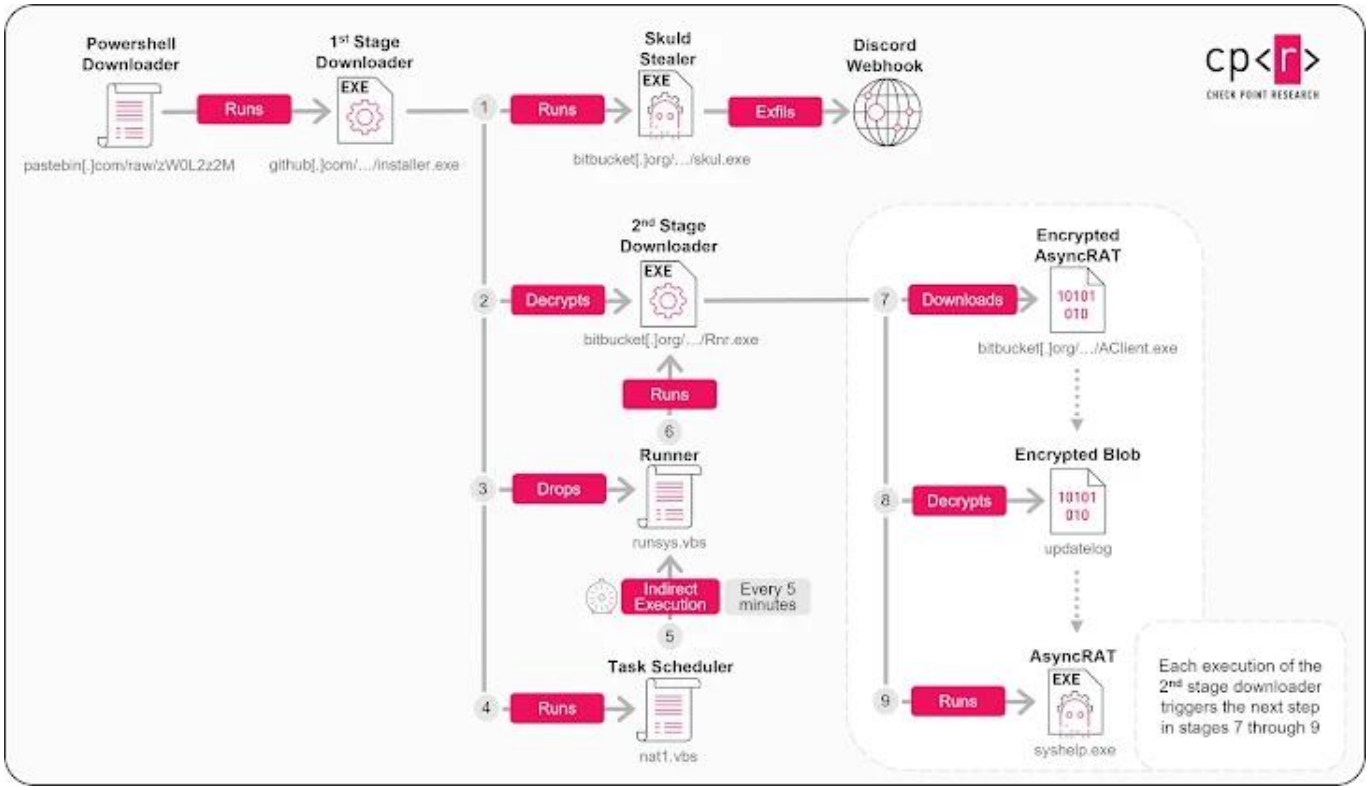
> Los detalles de esta campaña surgen poco más de un mes después de que la misma empresa de ciberseguridad revelara otra campaña de phishing sofisticada que aprovechaba enlaces de invitación personalizados ya expirados para atraer a los usuarios a un servidor de Discord, donde se les indicaba visitar un sitio web falso para verificar la propiedad de su cuenta, lo que resultaba en el robo de sus activos digitales al conectar sus monederos.

Aunque Discord permite crear enlaces de invitación temporales, permanentes o personalizados (vanity), la plataforma impide que otros servidores legítimos reclamen enlaces previamente expirados o eliminados. Sin embargo, Check Point descubrió que al crear enlaces personalizados es posible reutilizar códigos de invitación caducados e incluso,

en algunos casos, códigos permanentes eliminados.

> Esta posibilidad de reutilizar códigos de invitación expirados o eliminados mediante enlaces personalizados abre la puerta al abuso, permitiendo que los atacantes los reclamen para sus propios servidores maliciosos.
>
> *"Esto representa un riesgo grave: los usuarios que sigan enlaces de invitación previamente confiables (por ejemplo, publicados en sitios web, blogs o foros) pueden ser redirigidos sin saberlo a servidores falsos de Discord creados por actores maliciosos,"* advirtió Check Point.

El secuestro de enlaces de invitación en Discord, en resumen, consiste en tomar el control de enlaces compartidos originalmente por comunidades legítimas y usarlos para redirigir a los usuarios a servidores maliciosos. Una vez dentro, se les solicita completar un proceso de verificación para obtener acceso completo al servidor, lo cual incluye autorizar un bot que los lleva a un sitio falso con un botón destacado que dice "Verificar".



Es en este punto donde los atacantes llevan el engaño al siguiente nivel, utilizando la conocida táctica de ingeniería social ClickFix para inducir a los usuarios a infectar sus sistemas bajo el pretexto de una verificación de identidad.

En concreto, al hacer clic en el botón “Verificar”, se ejecuta de manera encubierta un código JavaScript que copia un comando de PowerShell al portapapeles del sistema. Luego, se anima al usuario a abrir el cuadro de diálogo Ejecutar de Windows, pegar la llamada “cadena de verificación” (en realidad, el comando PowerShell) y presionar Enter para validar su cuenta.

> Pero en realidad, seguir estos pasos inicia la descarga de un script de PowerShell alojado en Pastebin, el cual recupera y ejecuta un primer descargador. Este componente inicial es el encargado de obtener desde

> un servidor remoto las cargas útiles finales: AsyncRAT y Skuld Stealer, que son ejecutadas en el sistema infectado.

En el centro de este ataque se encuentra un proceso de infección cuidadosamente diseñado por etapas, enfocado tanto en la precisión como en evitar la detección. Además, se incorporan mecanismos para evadir protecciones de seguridad, incluyendo verificaciones en entornos de prueba o sandbox.

> AsyncRAT, que brinda amplias capacidades de control remoto sobre los equipos comprometidos, utiliza una técnica llamada dead drop resolver para localizar su servidor de comando y control (C2), leyendo un archivo alojado en Pastebin.

El segundo componente malicioso es un ladrón de información programado en Golang, descargado desde Bitbucket. Este está diseñado para robar datos sensibles de usuarios en Discord, distintos navegadores, monederos de criptomonedas y plataformas de videojuegos.

> Skuld también tiene la capacidad de extraer frases semilla y contraseñas de monederos como Exodus y Atomic. Lo hace mediante una técnica llamada inyección de monedero, que sustituye archivos legítimos de las aplicaciones por versiones maliciosas descargadas desde GitHub. Cabe destacar que un enfoque similar fue utilizado recientemente por un paquete malicioso de npm llamado `pdf-to-office`.

El ataque también utiliza una versión modificada de una herramienta de código abierto conocida como ChromeKatz, diseñada para evadir las protecciones de cifrado asociadas a las aplicaciones de Chrome. La información recopilada es

enviada a los atacantes mediante un webhook de Discord.

> El uso de servicios legítimos en la nube —como GitHub, Bitbucket, Pastebin y Discord— tanto para entregar las cargas útiles como para extraer los datos, permite que los atacantes pasen desapercibidos al camuflar su actividad dentro del tráfico normal. Discord ha desactivado desde entonces el bot malicioso, interrumpiendo así la cadena de ataque.

Check Point también reportó haber identificado otra campaña vinculada al mismo grupo de atacantes, en la cual se distribuye el cargador en forma de una herramienta alterada para desbloquear videojuegos pirateados. Este programa malicioso, también alojado en Bitbucket, ha sido descargado 350 veces.

> Se ha determinado que la mayoría de las víctimas de estas campañas se encuentran en Estados Unidos, Vietnam, Francia, Alemania, Eslovaquia, Austria, Países Bajos y Reino Unido.

Estas revelaciones representan un nuevo ejemplo del modo en que los ciberdelincuentes están enfocando sus ataques en plataformas sociales populares como Discord, cuya red de distribución de contenido (CDN) ya ha sido aprovechada en el pasado para alojar malware.

> *“Esta campaña demuestra cómo una función aparentemente inofensiva del sistema de invitaciones de Discord —la reutilización de códigos de invitación expirados o eliminados mediante enlaces personalizados— puede convertirse en un vector de ataque muy efectivo. Al secuestrar enlaces legítimos, los atacantes logran redirigir de forma silenciosa a los usuarios desprevenidos hacia servidores de Discord maliciosos»,* afirmaron

los investigadores.

“La selección de cargas útiles, incluyendo un ladrón especializado en criptomonedas, sugiere que el objetivo principal de los atacantes son los usuarios del ecosistema cripto, impulsados por fines económicos.”