Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°014	Fecha: 16-01-2024
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los Piratas Informáticos Abusan De GitHub Para Alojar Infraestructura Maliciosa		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

GitHub se ha convertido en una plataforma importante que los ciberdelincuentes utilizan para diversos métodos de ataque. Esto se debe a que GitHub se considera tráfico legítimo, que los actores de amenazas pueden aprovechar para mezclarse con otro tráfico de red legítimo. Sin embargo, se espera que aumenten los ciberataques y existen altas posibilidades de que surjan nuevos vectores de riesgo de terceros.

Github es un portal creado para alojar el código de las aplicaciones de cualquier desarrollador, y que fue comprada por Microsoft en junio del 2018. La plataforma está creada para que los desarrolladores suban el código de sus aplicaciones y herramientas, y que como usuario no sólo puedas descargarte la aplicación, sino también entrar a su perfil para leer sobre ella o colaborar con su desarrollo.

2. DETALLES:

Según un informe compartido por Recorded Future, "La utilización de los servicios de GitHub para infraestructura maliciosa permite a los adversarios mimetizarse con el tráfico de red legítimo, eludiendo a menudo las defensas de seguridad convencionales y complicando el rastreo de la infraestructura aguas arriba y la atribución del actor".

Se recomienda a las organizaciones que inviertan recursos en comprender el abuso de Github y los repositorios de código, lo que podría proporcionar más información sobre los ataques.

Según el informe compartido con Cyber Security News, casi todos los actores de amenazas utilizan GitHub para evadir la detección, reducir costos y reducir los gastos operativos. Sin embargo, los esquemas de infraestructura principal se han cambiado a entrega de carga útil, DDR, C2 completo y exfiltración.

Entre ellos, la entrega de carga útil es el esquema más frecuente debido a su sencilla implementación. Aunque esto ofrece una gran cantidad de beneficios, existe una desventaja para los actores de amenazas al usar GitHub para la entrega de carga útil. Los riesgos incluyen exposición no deseada, fuga de información operativa y muchos otros.

Dead Drop Resolving es la segunda técnica más común que utiliza la plataforma GitHub. DDR tiene un riesgo mínimo de eliminación de datos de la plataforma, lo que proporciona un excelente lugar para colocar archivos maliciosos, ya que las plataformas tipo GitHub tienen desafíos para detectar archivos detrás de direcciones o cadenas publicadas sin más contexto.

También se ha descubierto que el comando y control están aumentando con las plataformas GitHub, pero la implementación completa de C2 en GitHub es poco común y sólo la realizan APT. Se especula que la razón detrás son las limitaciones funcionales en el uso de los servicios de GitHub.

En cuanto a la exfiltración, también es menos común en comparación con otros métodos. Esto podría deberse a limitaciones de tamaño y almacenamiento, alternativas efectivas, problemas de costos y problemas de detectabilidad.

3. RECOMENDACIONES:

- Practicar una higiene estricta de las contraseñas. Utilizar contraseñas únicas y complejas para todas las cuentas y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- No hacer clic en enlaces sospechosos ni descargue archivos adjuntos de fuentes desconocidas.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.

Fuente de Información:	• hxxps://gbhackers.com/hackers-abuse-github-to-host-malicious-infrastructure/ • hxxps://blogs.masterhacks.net/noticias/hacking-y-ciberdelitos/los-actores-de-amenazas-estan-abusando-cada-vez-mas-de-github-con-fines-maliciosos/