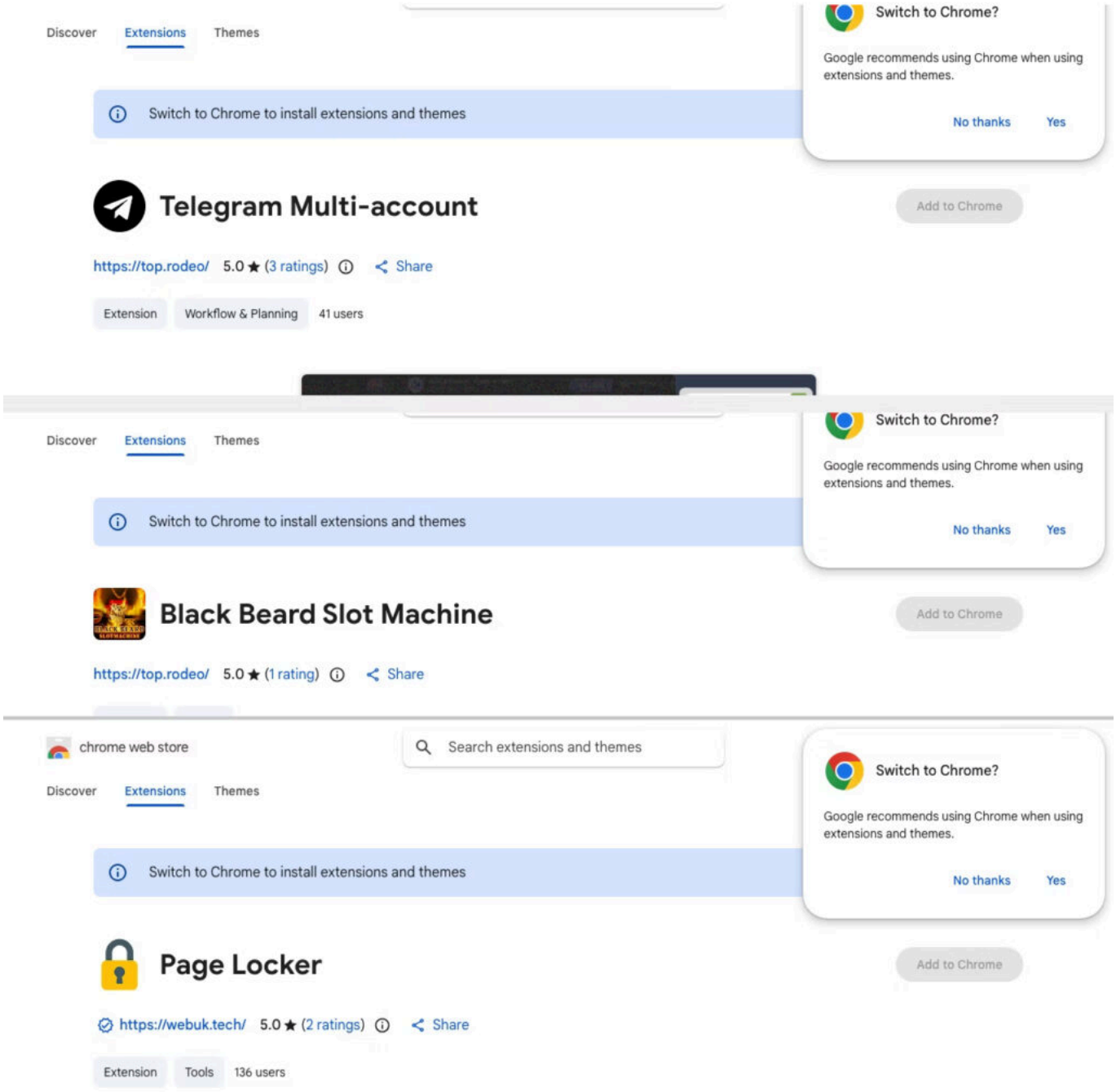
Investigadores de ciberseguridad han identificado una nueva campaña en la que un conjunto de 108 extensiones de Google Chrome se comunica con la misma infraestructura de comando y control (C2), con el objetivo de recolectar datos de usuarios y facilitar abusos a nivel del navegador mediante la inserción de anuncios y código JavaScript arbitrario en cada página web visitada.

De acuerdo con Socket, las extensiones (lista completa aquí) se publicaron bajo cinco identidades distintas — Yana Project, GameGen, SideGames, Rodeo Games e InterAlt — y en conjunto han alcanzado alrededor de 20,000 instalaciones en la Chrome Web Store.

«Las 108 extensiones envían credenciales robadas, identidades de usuario y datos de navegación a servidores controlados por un mismo operador», señaló el investigador de seguridad Kush Pandya en un análisis.

De ellas, 54 complementos roban la identidad de cuentas de Google mediante OAuth2, 45 extensiones incluyen una puerta trasera universal que abre URLs arbitrarias al iniciar el navegador, y las restantes llevan a cabo diversas acciones maliciosas –

- Exfiltran sesiones de Telegram Web cada 15 segundos
- Eliminan encabezados de seguridad de YouTube y TikTok (como Content Security Policy, X-Frame-Options y CORS) e insertan superposiciones de apuestas y anuncios
- Inyectan scripts en todas las páginas que visita el usuario
- Redirigen todas las solicitudes de traducción a través del servidor del atacante



Para aparentar legitimidad, las extensiones detectadas se hacen pasar por clientes de barra lateral de Telegram, juegos de tragamonedas y Keno, mejoras para YouTube y TikTok,

herramientas de traducción de texto y utilidades para páginas web. Las funciones anunciadas son variadas para atraer a más usuarios, aunque todas comparten la misma infraestructura interna.

Sin que los usuarios lo sepan, el código malicioso que se ejecuta en segundo plano recopila información de sesión, inserta scripts arbitrarios y abre enlaces definidos por el atacante.

Algunas de las extensiones identificadas incluyen –

Telegram Multi-account (ID: obifanppcpchlehkjipahhphbcbjekfa), que extrae el token user_auth utilizado por Telegram Web y envía los datos a un servidor remoto. También puede sobrescribir el almacenamiento local (localStorage) con información de sesión proporcionada por el atacante y forzar la carga de la aplicación de mensajería, sustituyendo efectivamente la sesión activa de la víctima por otra controlada por el atacante.

Web Client for Telegram – Teleside (ID: mdcfennpfgkngnibjbpnpaafcjnhcjno), que elimina los encabezados de seguridad de Telegram e inyecta scripts para robar sesiones.

Formula Rush Racing Game (ID: akebbllmckjphjiojeioooidhnddnplj), que roba la identidad de la cuenta de Google del usuario la primera vez que la víctima hace clic en el botón de inicio de sesión, incluyendo datos como correo electrónico, nombre completo, URL de la foto de perfil y el identificador de la cuenta.

«Cinco extensiones utilizan la API declarativeNetRequest de Chrome para eliminar encabezados de seguridad de los sitios objetivo antes de que la página cargue», indicó Socket. «Las 108 extensiones maliciosas comparten el mismo backend, alojado en 144.126.135[.]238».

Actualmente no se sabe quién está detrás de estas extensiones que incumplen las políticas. No obstante, un análisis del código fuente ha revelado comentarios en idioma ruso en varios de estos complementos.

Se recomienda a los usuarios que hayan instalado alguna de estas extensiones eliminarlas de inmediato y cerrar todas las sesiones de Telegram Web desde la aplicación móvil de Telegram.