Campañas maliciosas de la extensión de navegador DarkSpectre han sido expuestas luego de afectar a 8.8 millones de personas en todo el mundo

El actor de amenazas responsable de dos campañas maliciosas de extensiones de navegador, conocidas como ShadyPanda y GhostPoster, ha sido vinculado a una tercera operación denominada DarkSpectre, la cual ha afectado a 2.2 millones de usuarios de Google Chrome, Microsoft Edge y Mozilla Firefox.

Se estima que esta actividad corresponde a un actor chino al que la empresa Koi Security sigue bajo el alias DarkSpectre. En conjunto, las campañas han impactado a más de 8.8 millones de usuarios a lo largo de un período superior a siete años.

ShadyPanda fue expuesta por primera vez por la compañía de ciberseguridad a inicios de este mes, al detectarse que apuntaba a usuarios de los tres navegadores con el fin de robar datos, secuestrar consultas de búsqueda y cometer fraude de afiliados. Se determinó que afectó a 5.6 millones de usuarios, incluidos 1.3 millones de víctimas recién identificadas, derivadas de más de 100 extensiones asociadas al mismo grupo.

Entre ellas se encuentra un complemento para Edge llamado *"New Tab – Customized Dashboard"*, el cual incorpora una bomba lógica que espera tres días antes de activar su comportamiento malicioso. Esta activación retardada busca aparentar legitimidad durante el período de revisión y así lograr su aprobación.

Actualmente, nueve extensiones permanecen activas, junto con 85 "durmientes" inactivos, que son benignos en apariencia y están diseñados para atraer usuarios antes de ser convertidos en armas mediante actualizaciones maliciosas. Según Koi, en algunos casos estas actualizaciones se introdujeron después de más de cinco años.

La segunda campaña, GhostPoster, se centra principalmente en usuarios de Firefox, a quienes ataca mediante utilidades aparentemente inofensivas y herramientas VPN. Estas extensiones distribuyen código JavaScript malicioso destinado a secuestrar enlaces de afiliados, insertar código de rastreo y llevar a cabo fraude de clics y publicidad. Investigaciones adicionales revelaron más complementos, incluida una extensión de Google Translate para Opera, publicada por *"charliesmithbons"*, con casi un millón de instalaciones.

La tercera campaña atribuida a DarkSpectre es The Zoom Stealer, que involucra 18 extensiones distribuidas en Chrome, Edge y Firefox. Estas se enfocan en inteligencia de reuniones corporativas, recopilando datos como URLs de reuniones con contraseñas incrustadas, IDs, temas, descripciones, horarios programados y estados de registro.

A continuación se presenta la lista de extensiones identificadas junto con sus respectivos ID:

Google Chrome

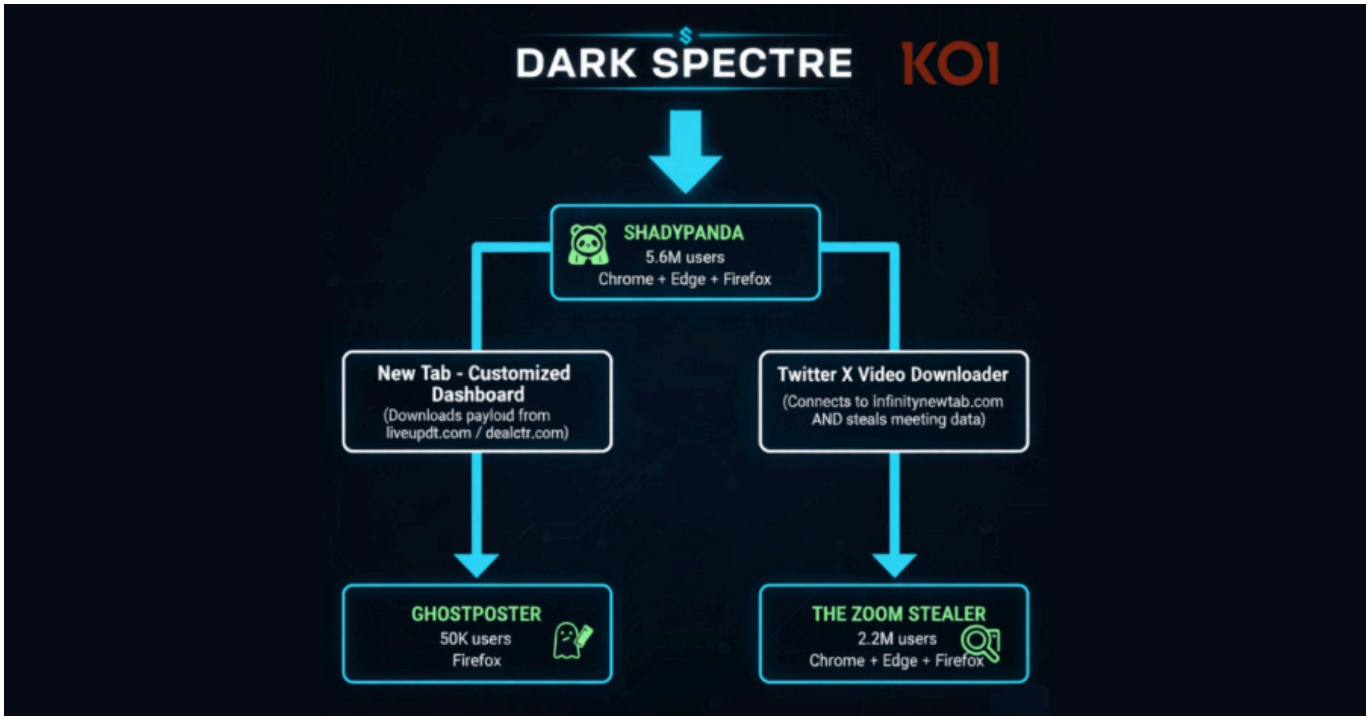
- Chrome Audio Capture (kfokdmfpdnokpmpbjhjbcabgligoelgp)
- ZED: Zoom Easy Downloader (pdadlkbckhinonakkfkdaadceojbekep)
- X (Twitter) Video Downloader (akmdionenlnfcipmdhbhcnkighafmdha)
- Google Meet Auto Admit (pabkjoplheapcclldpknfpcepheldbga)
- Zoom.us Always Show *"Join From Web"* (aedgpiecagcpmehhelbibfbgpfiafdkm)
- Timer for Google Meet (dpdgjbnanmmlikideilnpfjjdbmneanf)
- CVR: Chrome Video Recorder (kabbfhmcaaodobkfbnnehopcghicgffo)
- GoToWebinar & GoToMeeting Download Recordings (cphibdhgbdoekmkkcbbaoogedpfibeme)
- Meet auto admit (ceofheakaalaecnecdkdanhejojkpeai)
- Google Meet Tweak (Emojis, Text, Cam Effects) (dakebdbeofhmlnmjlmhjdmmjmfohiicn)
- Mute All on Meet (adjoknoacleghaejlggocbakidkoifle)
- Google Meet Push-To-Talk (pgpidfocdapogajplhjofamgeboonmmj)
- Photo Downloader for Facebook, Instagram, + (ifklcpoenaammhnoddgedlapnodfcjpn)
- Zoomcoder Extension (ebhomdageggjbmomenipfbhcjamfkmbl)
- Auto-join for Google Meet (ajfokipknlmjhcioemgnofkpmdnbaldi)

Microsoft Edge

- Edge Audio Capture (mhjdjckeljinofckdibjiojbdpapoecj)

Mozilla Firefox

- Twiter X Video Downloader ({7536027f-96fb-4762-9e02-fdfaedd3bfb5}, publicado por *“invaliddejavu”*)
- x-video-downloader (xtwitterdownloader@benimaddonum.com, publicado por *“invaliddejavu”*)



Tal como lo sugieren los nombres de las extensiones, la mayoría están diseñadas para imitar herramientas legítimas de aplicaciones de videoconferencia empresariales como Google Meet, Zoom y GoTo Webinar, con el objetivo de extraer enlaces de reuniones, credenciales y listas de participantes en tiempo real mediante una conexión WebSocket.

Además, estas extensiones son capaces de recopilar información sobre ponentes y anfitriones de seminarios web, incluyendo nombres, cargos, biografías, fotos de perfil y afiliaciones corporativas, así como logotipos, material promocional y metadatos de las sesiones, cada vez que un usuario accede a una página de registro de un webinar desde el navegador con alguna de ellas instalada.

Se ha determinado que estos complementos solicitan acceso a más de 28 plataformas de videoconferencia, entre ellas Cisco WebEx, Google Meet, GoTo Webinar, Microsoft Teams y Zoom, independientemente de si realmente necesitaban dicho acceso para funcionar.

"Esto no es fraude al consumidor; se trata de infraestructura de espionaje corporativo", afirmaron los investigadores Tuval Admoni y Gal Hachamov. *"Zoom Stealer representa algo mucho más específico: la recolección sistemática de inteligencia sobre reuniones corporativas. Los usuarios recibieron exactamente lo que se anunciaba. Las extensiones generaron confianza y obtuvieron reseñas positivas. Mientras tanto, la vigilancia operaba de forma silenciosa en segundo plano"*.

La empresa de ciberseguridad indicó que la información recopilada podría utilizarse para impulsar actividades de espionaje empresarial, ya sea mediante la venta de los datos a otros actores maliciosos o facilitando operaciones de ingeniería social y suplantación de identidad a gran escala.

Los vínculos de la operación con China se sustentan en varios indicios: el uso constante de servidores de comando y control (C2) alojados en Alibaba Cloud, registros de Internet Content Provider (ICP) asociados a provincias chinas como Hubei, artefactos de código con cadenas y comentarios en idioma chino, así como esquemas de fraude dirigidos específicamente a plataformas de comercio electrónico chinas como JD.com y Taobao.

"Es probable que DarkSpectre tenga actualmente más infraestructura activa: extensiones que parecen completamente legítimas porque, por ahora, lo son", señaló Koi. *"Aún se encuentran en la fase de construcción de confianza, acumulando usuarios, obteniendo insignias y esperando"*.