LayerX publicó su informe anual de seguridad del navegador en el que la empresa destaca los riesgos de seguridad del navegador que fueron más destacados en 2022. El informe también incluye predicciones y recomendaciones para 2023.

El informe se centra en los entornos empresariales, pero varios de sus puntos clave se aplican también a los entornos domésticos y de pequeñas empresas. Las amenazas de seguridad del navegador de 2022 constituyen la mayor parte del documento, pero los usuarios también encuentran predicciones, recomendaciones y una descripción general mensual interesante de los principales eventos de seguridad en el informe.

Las nueve principales amenazas que LayerX identificó en 2022 fueron las siguientes:

- Ataques de phishing por medio de dominios de alta reputación
- Distribución de malware por medio de sistemas de intercambio de archivos
- Fuga de datos por medio de los perfiles personales del navegador
- Navegadores obsoletos
- Contraseñas vulnerables
- Dispositivos no administrados
- Extensiones de alto riesgo
- Sombra SaaS
- Omisión de MFA con ataques AiTM

Algunos de estos son bastante claros, otros pueden requerir una explicación. Para los ataques de phishing, los investigadores descubrieron que los hackers alojan URL de phishing en plataformas SaaS legítimas a un ritmo muy alarmante.

La tasa de ataques de phishing que usan estas plataformas legítimas ha aumentado un 1100% en comparación con 2021, según un estudio de Palo Alto Networks.

LayerX realizó pruebas sobre qué tan bien los navegadores y las herramientas de seguridad de la red se protegieron contra los sitios de phishing de un día. Según la prueba, el navegador con mejor rendimiento tuvo una tasa de captura de solo el 36%. El software de

seguridad de red bloqueó el 48% de las amenazas.

De forma similar, el malware se distribuye a través de servicios sancionados como Google Drive y Microsoft OneDrive, para superar los bloqueos que pueden existir para servicios y sitios menos conocidos.

Un análisis de la fuga de datos en los navegadores concluyó que el 29% de los usuarios conectaron los navegadores del trabajo a sus perfiles personales y que el 5.8% de las identidades quedaron expuestas en las filtraciones de datos.

Los navegadores obsoletos son otra amenaza para la seguridad, según el informe de LayerX. Un análisis de 500 navegadores Chrome reveló que un buen número estaba críticamente desactualizado o era vulnerable a ataques de 1 día.

Las contraseñas débiles y la reutilización de contraseñas siguen siendo problemas importantes. Según el informe de LayerX, el 29% de los usuarios utiliza contraseñas débiles o medianas, y el 11% de los usuarios reutiliza las contraseñas de forma regular. La empresa notó que el 29% de los perfiles de navegador eran personales y estaban configurados para sincronizarse.

Las extensiones de navegador web son otro vector de ataque, ya que *«pueden otorgar permisos excesivos una vez instaladas».* Un estudio reciente de Incogni encontró que casi la mitad de las extensiones de navegador analizadas presentaban un alto riesgo de seguridad o privacidad.

El informe incluye una descripción general de los aspectos más destacados de la seguridad del navegador del año 2022. Es una cuenta interesante que enumera los principales eventos de seguridad en 2022. Algunos de estos ataques involucraron, como el ataque del reproductor de video de enero de 2022 que robó información de tarjetas de crédito de más de cien sitios. Otros destacan los avances en seguridad, como el anuncio de los inicios de sesión sin contraseña por parte de las principales empresas tecnológicas en mayo o el fin de Internet Explorer en junio.

El informe concluye con cuatro predicciones y recomendaciones. Las predicciones incluyen que los navegadores web se convertirán en *«la principal superficie de ataque»,* que los ataques *«se basarán cada vez más en SaaS y menos en archivos»* y que las páginas web maliciosas *«se volverán más sofisticadas».*