TECNOLOGÍA | SEGURIDAD INFORMÁTICA

**Usuarios y claves de 850 organismos argentinos, filtrados por hackers**

*Publican gratis credenciales de acceso "gob.ar" y "gov.ar", sitios apócrifos para consultar el padrón electoral, crackean el nuevo casco de VR de PlayStation y desarticulan el malware Snake. Infiltrados obtuvieron datos de Organismos de Estado, Ministerios y Poder Judicial.*

**Por Julián M. Zappia.  
Diplomatic Week.**

Un canal especializado de compra y venta de datos personales publicó una “combolist”, esto es, un archivo de texto con usuarios y contraseñas, con más de 100 mil credenciales de acceso.

Entre ellas, 2.155 pertenecen a agentes de Gobierno de cerca de 850 organismos argentinos. Están disponibles de manera gratuita.

Hay accesos de varias fuerzas de seguridad, AFIP, ANMAT, ministerios, fiscalías, el Poder Judicial y más.

No es la primera vez que ocurre una fuga de datos relacionada a organismos del Estado argentino: en octubre de 2020 la Dirección Nacional de Migraciones sufrió un ataque de ransomware que derivó en una publicación masiva de datos de ciudadanos.

Un año después, el RENAPER, que maneja los documentos de identidad, pasaportes y otros certificados sensibles, tuvo un acceso no autorizado que extrajo datos de 60 mil argentinos. Tres días después, el Ministerio de Salud denunció el caso adjudicando un ataque de phishing.

Este nuevo caso no tuvo cobertura mediática, pero representa un peligro para los usuarios afectados.

El caso se suma así a la larga lista de filtraciones relacionadas al Estado argentino, uno de los más afectados a nivel regional por este tipo de incidentes.

**Web de phishing para consultar el padrón.**

Faltan cerca de tres meses para las elecciones Primarias Abiertas Simultáneas y Obligatorias (PASO) en Argentina: serán el 13 de agosto. Las generales, el 22 de octubre. A partir de la cercanía con estas fechas, ya empezaron a circular sitios apócrifos para consultar el padrón electoral.

Merlax advirtió que el problema podría multiplicarse de acá a las PASO:

Un tema grave de todos estos sitios es que, si pagan, pueden promocionarlos en Google Ads. Como ya trató SecOps, es un problema que el buscador más famoso del mundo todavía no resuelve: que cualquier estafador pueda pagar para aparecer primero en la lista de resultados.

Merlax no descartó que más adelante haya otros medios de propagación como puede ser WhatsApp, SMS o correos electrónicos.

Este tipo de sitios se pueden denunciar ante el Equipo de Respuesta de Emergencias Informáticas (CERT).

**Intervención del FBI.**

El FBI logró intervenir “Snake”, un software malicioso utilizado por espías rusos de élite. La noticia recorrió titulares del mundo porque es un ladrillo más en la pared de la ciberguerra entre dos potencias mundiales.

Expertos técnicos del FBI identificaron y deshabilitaron el malware utilizado por el servicio de seguridad ruso FSB contra un número no revelado de computadoras estadounidenses. "Evaluamos esto como su principal herramienta de espionaje", aseguró uno de los funcionarios estadounidenses a los periodistas antes del anuncio.

“Turla”, como se identificó al célebre grupo de hackers rusos que estuvo detrás de este malware, ha estado activo por dos décadas, aseguró el FBI.

Rusia no respondió las solicitudes de comentarios de medios occidentales y negó todo tipo de vínculo con operaciones de ciber-espionaje.

**El navegador Firefox.**

Mozilla lanzó la versión 113 de su navegador Firefox. Uno de los cambios más importantes es que el generador de contraseñas integrado de Firefox viene con una importante mejora: ahora permite agregar caracteres especiales a las claves aleatorias.

Esto permite a Firefox generar contraseñas que superarán la mayoría de las pruebas de complejidad de contraseñas, cosa que antes no hacía.

Además, las ventanas privadas ahora “protegen aún mejor a los usuarios bloqueando las cookies de terceros y el almacenamiento de rastreadores de contenidos”, aseguran.

**El casco de realidad virtual PlayStation VR2.**

El casco de Realidad Virtual de PlayStation, uno de los más importantes del rubro, ya fue crackeado: el hardware de autenticación puede ser “puenteado”, según contó en Twitter un desarrollador de software.

Aunque, según explicó, “todavía hay mucho trabajo por hacer”, esto significa que por ejemplo se lo podría hacer funcionar en una PC en lugar de una consola.

No hay mucha más información al respecto más que la confirmación del investigador de que las restricciones que Sony establecidas de fábrica ahora pueden ser vulneradas.

**Los dominios de DDoS desarticulados.**

El Departamento de Justicia de EE.UU. (DOJ) anunció que dio de baja 13 dominios usados para cometer ataques de DDoS, una maniobra que satura las conexiones para impedir el acceso a usuarios legítimos.

Las autoridades explicaron que diez de los 13 dominios incautados esta semana son reencarnaciones de portales DDoS retirados anteriormente en diciembre de 2022. En aquel momento, Europol y el FBI retiraron un lote de 48 dominios utilizados para ataques DDoS y detuvieron a seis sospechosos.

Sobre este punto, es interesante ver cómo los cibercriminales reutilizan herramientas previas para cometer ataques, explicó recientemente Derek Manky, jefe de análisis de amenazas de Fortinet:

“Podríamos decir que están utilizando los principios de reducir, reutilizar y reciclar, pero en lugar de enfocarlos en el medio ambiente lo están adaptando con el código malicioso para permitir resultados criminales más exitosos. De hecho, en nuestro análisis del malware más reportado para la segunda mitad de 2022, vimos que la mayor parte de los primeros puestos estaban ocupados por malware que tenía más de un año. Algunos de ellos, como Lazarus, existen desde hace más de 10 años y son pilares de la historia de internet”.

Según el Departamento de Justicia estadounidense, cuatro de esos seis sospechosos se declararon culpables y está previsto que sean condenados inmediatamente.