csirt-bcf
equipo de respuesta a incidentes de ciberseguridad
BioCubaFarma

MALWARE EN VIDEOJUEGOS

CSIRT-BCF

Contribuimos a su cultura sobre ciberseguridad.

¿CÓMO ME INFECTO?

Los ciberdelincuentes pueden inyectar un código malicioso en un juego legítimo, crear y distribuir sitios webs de bonificaciones, aplicaciones de juego falsas, programas complementarios, actualizaciones, trucos o mods (modificaciones que se instalan sobre el juego básico) que contengan un malware oculto en el archivo de descarga.

¿CÓMO FUNCIONAN?

Al descargar y ejecutar este tipo de archivos, el malware se instala en el sistema y realiza la función para la cual fue creado, trabajando en segundo plano, sin que el usuario se dé cuenta.
Algunos de estos archivos de descarga pueden no ser peligrosos en sí mismos, pero puede usarse para cargar otras amenazas en los dispositivos.

VÍAS DE DISTRIBUCIÓN

El malware viene disfrazado dentro de archivos descargables y enlaces falsos que son distribuídos a través de foros, correos electrónicos, sitios web no oficiales, redes sociales, chats de juegos, etc.

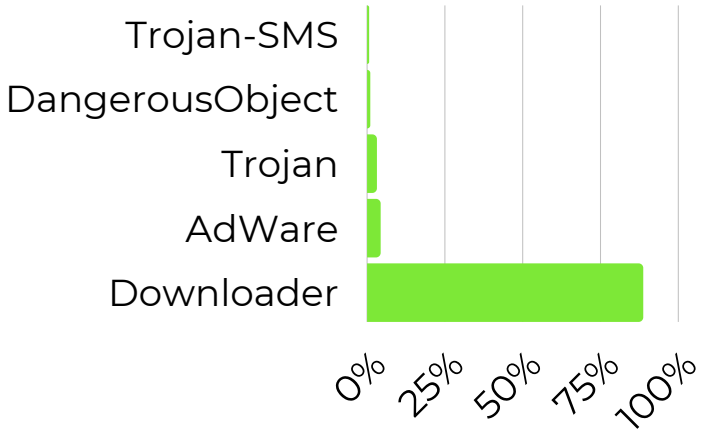
https://csirt.biocubafarma.cu/

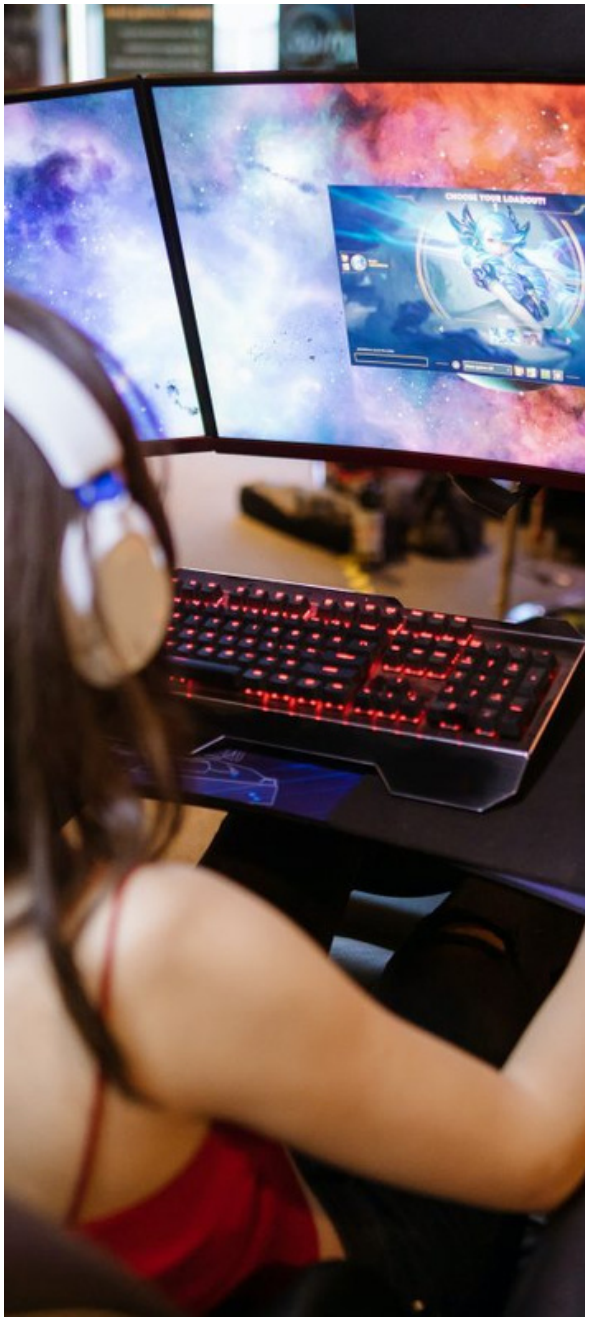
csirt-bcf
equipo de respuesta a incidentes de ciberseguridad BioCubaFarma

RIESGOS DE LOS JUEGOS EN LÍNEA

- Malware.
- Robo de identidad.
- Usurpación de cuentas.
- Filtraciones de datos .
- Ataques DDoS.
- Correos electrónicos de phishing.
- Acoso en línea.
- Scripting entre sitios.
- Spyware.
- Swatting y doxing.

AMENAZAS EN VIDEOJUEGOS (2022)





Juegos más utilizados como señuelos en los ataques dirigidos a la mayor cantidad de usuarios en 2022 según la empresa Kaspersky.

TOP 5 DE JUEGOS MÁS ATACADOS EN MÓVILES

1. Minecraft
2. Roblox
3. Grand Theft Auto (GTA)
4. PUBG
5. FIFA

TOP 10 DE JUEGOS MÁS ATACADOS EN PC

1. Minecraft
2. Roblox
3. Need for Speed
4. Grand Theft Auto (GTA)
5. Call of Duty
6. FIFA
7. The Sims
8. Far Cry
9. CS:GO
10. PUBG

csirt-bcf
equipo de respuesta a incidentes de ciberseguridad BioCubaFarma

SEGURIDAD PARA JUGADORES

- Usa contraseñas seguras y únicas para cada cuenta.
- Configure la autenticación en dos pasos (2FA).
- Realice descargas de fuentes legítimas.
- Esté atento a gastos ocultos y a las estafas potenciales.
- Manténgase alerta ante las campañas de phishing.
- Elimine del dispositivo el juego de manera segura.
- Verifique la autenticidad de cualquier sitio web que solicite sus credenciales.
- Mantenga su sistema operativo y otros softwares actualizados.
- No acceda a ningún enlace de sitios externos que le envíen desde el chat del juego, correo electrónico, redes sociales, etc.
- Utilice una solución antivirus que no relentice el dispositivo mientras juega.

> *Los jugadores pueden seguir disfrutando de esta actividad de forma segura, sólo tienen que seguir las mejores prácticas básicas de ciberseguridad.*

MARIA NAMESTNIKOVA
Jefa del Equipo de Investigación y Análisis Global de Rusia

REFERENCIAS

https://securelist.com/gaming-related-cyberthreats-2021-2022/107346/

https://latam.kaspersky.com/resource-center/threats/top-10-online-gaming-risks

https://tn.com.ar/tecno/juegos/2022/09/10/minecraft-y-the-sims-estan-entre-los-videojuegos-mas-usados-para-difundir-malware-entre-gamers/

https://csirt.biocubafarma.cu/