

Ciberdelincuencia juvenil: cómo evitar que los más chicos tomen el camino equivocado



Cuando se habla de la ciberdelincuencia y los niños, suele ser en el contexto de proteger a los más pequeños de los peligros online. Por ejemplo, asegurarse de que sus dispositivos cuenten con un software de control parental adecuado, de modo que no puedan acceder a contenido peligroso o inapropiado. O comprobar que tengan instalado un antimalware y que la privacidad esté configurada correctamente. **¿Pero qué pasa cuando el niño es el que resulta ser el “malo”?** ESET, compañía líder en detección proactiva de amenazas, desde su iniciativa Digipadres, que busca acompañar padres y docentes en el cuidado de los niños en Internet, analizan este fenómeno y acercan consejos para acompañar a los más pequeños en estos casos.

Esta situación se presenta de una forma más común de lo que se cree, entre otras cosas porque, a una edad temprana muchos niños aún no se dan cuenta de que sus actividades de “sombbrero negro” son ilegales (en comparación con las de “sombbrero blanco”, también conocidas como “hacking ético”). Por ejemplo, la alumna londinense Betsy Davies tenía solo siete años cuando demostró cómo hackear la computadora portátil de un desconocido a través de una red Wi-Fi pública no segura en solo 10 minutos. **Esto lo logró al buscar una guía en Internet. En ese momento se encontraron alrededor de 14.000 tutoriales de video solamente en YouTube.**

“La buena noticia es que, incluso si se sospecha que un menor puede estar utilizando sus habilidades tecnológicas con fines maliciosos, no es demasiado tarde para guiarlo hacia el camino correcto. Son muchas las vías legítimas para canalizar sus conocimientos cibernéticos y, en última instancia, ayudarlo a iniciar una carrera en ciberseguridad.”, comenta **Camilo Gutiérrez Amaya**, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

Los hackers de edad escolar son cada vez más numerosos, a medida que las herramientas y técnicas para cometer delitos cibernéticos se abaratan y son más accesibles. La **Agencia Nacional del Crimen** (NCA) del Reino Unido informó que los datos de su Unidad Nacional de Cibercrimen (NCCU) mostraron un aumento del 107% en los informes policiales de 2019 a 2020 de estudiantes que desplegaron ataques de DDoS (Ataque distribuido de denegación de servicio). La edad media de las derivaciones al equipo “Prevent” de la NCCU es, al parecer, de 15 años, y un reciente informe de la NCA reveló que se descubrieron niños de tan solo nueve años lanzando ataques de DDoS, aunque no se limitan a este tipo de ataque.

¿Cuáles son las señales de alarma?

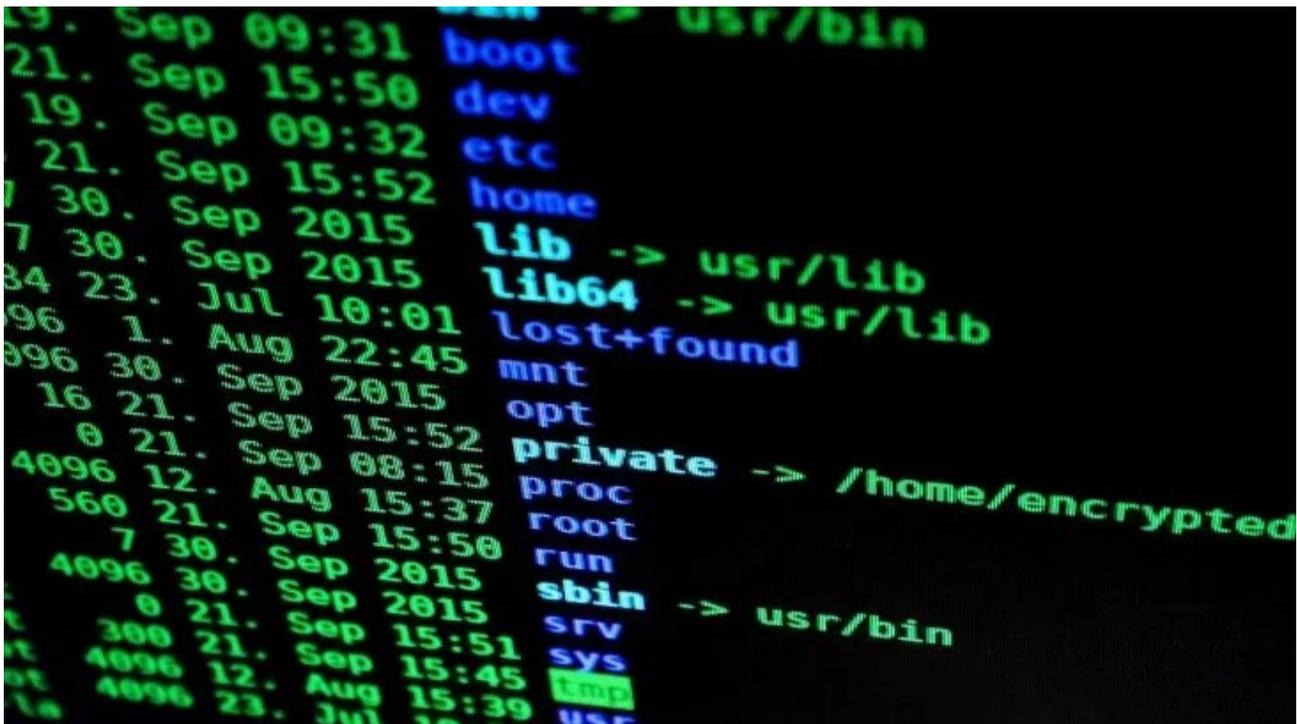
Desde ESET mencionan que es importante mantenerse alertas ante cualquier cambio en el comportamiento. Un estudio realizado por la Universidad Estatal de Michigan (MSU) puso de manifiesto algunos de los rasgos clave asociados a la ciberdelincuencia juvenil. Entre ellos se destacan:

- Bajo autocontrol.
- Relacionarse con pares; es decir, conocer a otros menores que también hackean.
- Tiempo dedicado a ver la televisión o a jugar con la computadora.
- Oportunidad; es decir, tener su propia computadora en una habitación privada, con una mínima supervisión de los padres.
- Acceso a un teléfono móvil desde una edad temprana.
- Participación en la piratería digital.

“También hay algunos indicios de que la actividad online de un niño o niña puede haberse descontrolado. Por ejemplo, puede hacer alusión a asuntos privados de los que no

debería tener conocimiento, lo que da la pauta de que estuvo leyendo correos electrónicos y mensajes personales de terceros; o puede hacer un esfuerzo extremo para proteger su propia privacidad, negándose a compartir sus inicios de sesión. Por supuesto, esto podría indicar simplemente que son niños siendo niños. De hecho, un interés temprano en algunos tipos de software, como las herramientas de pruebas de pentesting (se intenta vulnerar un sistema y ganar control del mismo para identificar sus puntos débiles y proponer acciones de mejora), podría ser más que bienvenido.”, agrega **Gutiérrez Amaya**.

Contar con un software de [control parental](#) en los dispositivos de los más pequeños ayuda a detectar las primeras señales de advertencia del hacking juvenil, como los intentos de acceder a sitios específicos de ciberdelincuencia, foros de hacking y otras zonas turbias de Internet. **Pero si se alcanzó un nivel elevado de conocimientos tecnológicos, es probable que puedan ser capaces de ocultar cualquier actividad de este tipo.**



Desde ESET recomiendan que si se detecta un comportamiento de este tipo se busque una alternativa positiva para sus habilidades. Hay programas de ciberseguridad para estudiantes en edad escolar con el fin de poner a prueba, perfeccionar y desarrollar sus habilidades. También hay concursos de hacking en los que todos los participantes pueden poner a prueba sus habilidades frente a los mejores del mundo, con la posibilidad de mostrar su talento. Pero **lo más importante es mantener las líneas de comunicación**

abiertas, interesarse por los pasatiempos de los más pequeños. En caso de tener una preocupación sobre su comportamiento se recomienda recordarles cuáles son los riesgos y alentarlos a buscar oportunidades más positivas para sus intereses.

En este sentido, **Javier Lombardi**, Mentor Educativo de **Argentina Cibersegura**, Asociación Civil que busca concientizar a la comunidad para crear un espacio digital más seguro, comenta: “Como adultos debemos ser conscientes de que nuestras reacciones, palabras y formas van modelando la de los niñas, niños y adolescentes. Nuestra intervención es necesaria, cada vez que veamos, escuchemos o tomemos contacto con una situación o una acción inapropiada, o que se esté realizando un desbalance en nuestra comunicación. De esta manera, estaremos gestionando el sistema de atención que luego veremos aprendido por niños, niñas y adolescentes, sirviendo así de STOP para cualquier comportamiento desajustado y que pueda generar un mal a otra persona, o a ellos mismos”.

Fuente: **Ámbito**