

Ciberseguridad: Malware por menos de 10 euros y en kits listos para usar: así se potencia la ciberdelincuencia desde la dark web

La reputación y la confianza son partes esenciales del comercio de los ciberdelincuentes, quienes han desplegado en la dark web un mercado que potencia la adquisición de kits de malware listos para usar a precios económicos, inferiores en muchos casos a los 10 euros.

El último informe de seguridad publicado por HP Wolf, La evolución de la ciberdelincuencia: por qué la Dark Web está sobrealimentando el panorama de las amenazas y cómo contraatacar, recoge la investigación realizada con Forensic Pathways sobre la dark web, en la que se rastrearon y analizaron más de 35 millones de mercados y mensajes de foros para entender cómo operan los ciberdelincuentes, cómo se ganan la confianza y cómo construyen su reputación.

Los resultados muestran que la ciberdelincuencia se está potenciando a través de kits de malware listos para usar (plug–and–play), que facilitan el lanzamiento de ataques. Ya que reducen la necesidad de conocimientos técnicos y experiencia para llevar a cabo ataques complejos y dirigidos; de hecho, sólo el 2 o el 3 por ciento de los autores de amenazas son programadores expertos.

El malware, además, es barato y fácil de conseguir. Más de tres cuartas partes (76%) de los anuncios de malware que aparecen, y el 91 por ciento de los exploits (el código que da a los atacantes el control de los sistemas aprovechando los fallos del software), se venden al por menor por menos de 10 euros. El coste medio de las credenciales del Protocolo de Escritorio Remoto comprometidas es de algo menos de 5 euros.

El informe también recoge que el 77 por ciento de los mercados de ciberdelincuentes analizados requieren una fianza de vendedor que puede costar hasta 3.000 euros. El 85 por ciento de ellos utilizan pagos en custodia, y el 92 por ciento tienen un servicio de resolución de conflictos de terceros.

Los ciberdelincuentes también intentan ir un paso por delante de las fuerzas de seguridad transfiriendo su reputación entre sitios web, ya que la vida media de un usuario o perfil que usa el navegador de Internet Tor para moverse por la dark web es de sólo 55 días.

Asimismo, se concluye con la investigación que los ciberdelincuentes se están centrando en la búsqueda de brechas en el software que les permitan conseguir un punto de apoyo y tomar el control de los sistemas, centrándose en los errores y vulnerabilidades conocidos en el software común.

Algunos ejemplos son el sistema operativo Windows, Microsoft Office, los sistemas de gestión de contenidos web, y los servidores web y de correo. Los kits que aprovechan las vulnerabilidades de los sistemas de nicho son los que alcanzan los precios más elevados (suelen oscilar entre 1.000 y 4.000 euros).

Las vulnerabilidades de día cero (las que aún no se conocen públicamente) se venden a decenas de miles de euros en los mercados de la dark web.

Fuente: *Cope*