Últimamente han crecido considerablemente los ataques de malware, especialmente con ramsonware, como WannaCry, que ha atacado sistemas en todo el mundo. Ahora, se sabe de un malware que es casi indetectable, por lo que podría seguir en el equipo aunque se formatee el disco duro.

LoJax es un rootkit UEFI, que según RedZone, puede resistir un formateo o cambio de disco duro. Debido a que el rootkit no se aloja en el sistema operativo, la mayoría de los antivirus no logran detectarlo ya que no analizan la UEFI.

Hasta ahora, se considera como uno de los rootkit más peligrosos y fue desarrollado por el grupo de hackers APT28, siendo uno de los más peligrosos del mundo. Han sido responsables por mucho malware que se ha detectado y por ataques a grandes empresas.

LoJax fue detectado en mayo pasado, pero no se tiene mucha información al respecto. Se está esparciendo por Europa y hasta ahora no se sabe cómo es capaz de propagarse por Internet.

Este rootkit cuenta con varios archivos binarios que recopilan información sobre el hardware y son capaces de parchear la UEFI con código malicioso. Una vez que la víctima se infecta, los atacantes tienen acceso total al sistema con más privilegios que el mismo sistema operativo, ya que infectan en tiempo real la memoria del sistema.