Cómo el mayor robo de datos en la historia de la CIA puso al descubierto su "laxa" seguridad

Por: Rusia Today
22/06/2020

Una unidad de la CIA especializada en el desarrollo de sofisticadas herramientas de piratería informática y armas cibernéticas sufrió en 2016 la peor pérdida de datos en la historia de la agencia, que se había centrado en aumentar su arsenal más que en mantenerlo seguro, y no disponía de un plan en caso de filtración o de robo de sus secretos. Así lo sugiere un informe interno preparado en 2017 y hecho público la semana pasada por el senador demócrata Ron Wyden.

El documento fue preparado por el grupo de trabajo WikiLeaks de la CIA en octubre de 2017 luego de una serie de filtraciones del portal fundado por Julian Assange que revelaron algunos de los activos de piratería más valiosos de la agencia de espionaje estadounidense.

Una seguridad "lamentablemente laxa"

Los autores del informe sostienen que las prácticas de seguridad cotidianas en el Centro de Inteligencia Cibernética de la CIA "se habían vuelto lamentablemente laxas".

Los empleados del centro "se centraron en la construcción de armas cibernéticas y no prepararon paquetes de mitigación en caso de que esas herramientas estuvieran expuestas", detalla el grupo de trabajo, agregando que "estas deficiencias fueron emblemáticas de una cultura que evolucionó a lo largo de los años y que con demasiada frecuencia dio prioridad a la creatividad y la colaboración a expensas de la seguridad".

Así, la mayoría de las armas cibernéticas sensibles no estaban compartimentadas, los usuarios compartían contraseñas de nivel de administrador de sistemas, no había controles efectivos de medios extraíbles (memoria USB), mientras que los datos históricos estaban disponibles para los usuarios de forma indefinida, detalla el informe.

El documento señala también que, debido a que los datos robados estaban en un sistema que carecía de

monitoreo de la actividad del usuario, la filtración no fue detectada hasta que WikiLeaks la anunció en marzo de 2017. "Si los datos hubieran sido robados para beneficio de un adversario estatal y no se hubieran publicado, aún podríamos desconocer la pérdida", admite el informe.

"La mayor pérdida de datos en la historia de la CIA"

Los investigadores consideran que esta fuga de proporciones históricas, conocida como Vault 7, es la "mayor pérdida de datos en la historia" de la agencia. No en vano, estiman que hasta 34 terabytes, o 2.200 millones de páginas, pueden haber sido robados y entregados a WikiLeaks por un empleado de la CIA. En total, el portal publicó descripciones completas de 35 herramientas, incluidos documentos internos de la CIA asociados con ellas.

El informe ya fue parcialmente desclasificado este año para el juicio de Joshua Schulte, exoficial de la CIA acusado de robar la información y proporcionársela a WikiLeaks. Schulte se declaró inocente, mientras que sus abogados argumentaron en el juicio que la seguridad de la red informática era tan pobre que cualquiera de los cientos de empleados o contratistas pudo haber tenido acceso a la misma información que el acusado. Un jurado no logró llegar a un veredicto en marzo sobre si Schulte le había entregado las herramientas a WikiLeaks.

El CIA se negó a hacer comentarios sobre el informe. No obstante, su portavoz, Timothy L. Barrett, aseguró que la agencia está trabajando para "incorporar las mejores tecnologías de su clase para mantenerse a la vanguardia y defenderse de las amenazas en constante evolución".