Smocze oczy kamer marki Hikvision

14 listopada 2022

W maju 2021, kolejna audycja programu „Raport” na kanale włoskiej telewizji RAI 3, w relacji zatytułowanej „Oko smoka”, ujawniła nieprawidłowości dotyczące kulis funkcjonowania kamer chińskiej marki Hikvision w systemie monitoringu video kompleksów włoskiej telewizji państwowej RAI. Po zakończeniu programu, do redakcji napłynęły liczne doniesienia, w tym jedno szczególnie niepokojące. Okazało się, że podobna anomalia dotknęła również lotniska Fiumicino pod Rzymem – największego lotniska we Włoszech.

1 kwietnia 2015 roku, administrator ds. bezpieczeństwa IT zorientował się, że ponad 100 kamer na terenie lotniska działa nieprawidłowo, więc wysłał wewnętrzną relację do swych zwierzchników. Dokument, w którego posiadanie wszedł „Report”, ostrzegał o poważnym problemie dotyczącym funkcjonowania kamer Hikvision, które próbują zarejestrować się na zewnętrznym serwerze o nieznanym (po dzień dzisiejszy) adresie IP. I tak w ciągu godziny odnotowano 11 tysięcy prób połączenia. Wciąż nie jest znany tego cel: może to być chęć przekazania danych lub umożliwienie komuś kontroli nad systemem monitoringu wizyjnego w strategicznym punkcie we Włoszech.

Hikvision Italia jest w posiadaniu holdingu europejskiego, który z kolei jest własnością chińskiej firmy-matki. Dyrektorzy spółki działającej na terenie Włoch są obywatelami Chin. Kontrola nad Hikvision jest w rękach CETC – chińskiej, państwowej firmy, która zajmuje się tworzeniem oprogramowania wojskowego, infrastruktury obronnej oraz broni elektronicznej. Krótko mówiąc, Hikvision – w 46% jest w rękach giganta ściśle związanego z militarnym kompleksem chińskim, a jego

administratorem jest parlamentarzysta Komunistycznej Partii Chin.

Relacja została również przekazana GSG, włoskiej firmie, która zarządzała oprogramowaniem systemu monitoringu. „Problem nie zależał od oprogramowania, ale od tego, że kamery próbowały skontaktować się z serwerem i próbowały otworzyć port, aby się wydostać" – powiedział mikrofonom „Reportu" Antonmarco Catania, prezes GSG Italia. Zainterweniował wtedy firewall lotniska. Z tego co wiemy, zdjęcia nie nie zostały przesłane. Być może był to atak na serwery w celu rozbicia systemów lotniska". Istnieje zatem podejrzenie, że sieć kamer może być wykorzystywana jako botnet do przeprowadzania cyberataków – co oznacza, że kamery są najpierw „infekowane", a następnie zdalnie – bez wiedzy producenta i użytkownika – wykorzystywane do ataków na inne sieci lub systemy komputerowe na lotnisku.

Jak zauważa „Report", kilka dni temu firma Fortinet zajmująca się cyberbezpieczeństwem odkryła, że tysiące kamer Hikvision zostało poddanych cyberatakom przez tzw. botnet, czyli sieć robotów, która jest wykorzystywana przez hakerów do wykradania informacji wrażliwych lub atakowania miejsc strategicznych.

Dziennikarze „Reportu" przeprowadzili eksperyment z kamerami, które codziennie monitorują wejścia pracowników RAI. Wraz z Francesco Zorzim, konsultantem-ekspertem w dziedzinie cyberbezpieczeństwa, przeniknęli do systemu nadzoru video RAI, aby zrozumieć, co dzieje się z danymi przechwyconymi przez kamery za każdym razem, gdy uda im się połączyć z siecią. Odkrycie bynajmniej nie było uspokajające, bo kamery rozmawiają ze sobą, przesyłają sobie dane, a jeśli są podłączone do Internetu, otwierają połączenie z podmiotem zewnętrznym, tj. serwerem znajdującym się najpierw w USA, a potem tym w Chinach – w regionie, w którym siedzibę ma produkująca je firma Hikvision.

W Wielkiej Brytanii, ministerstwo obrony zdecydowało, że nie będzie instalować kamer Hikvision w newralgicznych miejscach. Od roku 2020, w USA zabronione jest instalowanie kamer w miejscach federalnych bez zezwolenia ministerstwa obrony, a oni zabronili instalacji kamer Hikvision, Dahua i Huawei. „W USA bezpieczeństwo narodowe pozwala na tworzenie „list proskrybowanych" w sektorach zaawansowanych technologicznie" – powiedział „Reportowi" Roberto Baldoni, dyrektor Narodowej Agencji Bezpieczeństwa Cybernetycznego. „W Europie tego nie ma. W Europie tworzone są wyłącznie ogólne przepisy dotyczące certyfikacji w zakresie bezpieczeństwa cybernetycznego".

Na podstawie: RAI.it [1] [2]
Źródło zagraniczne: Startmag.it
Źródło polskie: BabylonianEmpire.wordpress.com