Cyberdefence 24

aut. Szymon Palczewski 27.05.2019

AMERYKAŃSKIE MIASTO SPARALIŻOWANE. NARZĘDZIE NSA BRONIĄ HAKERÓW

Przez prawie trzy tygodnie Baltimore zmagało się z skutkami cyberataku, który zatrzymał działanie tysięcy komputerów oraz zablokował adresy e-mail. Na skutek działań hakerów miasto zostało sparaliżowane. Niemożliwe było prowadzenie transakcji internetowych, komunikacji z państwowymi organami, a także korzystanie z wielu innych usług.

Sfrustrowani mieszkańcy miasta nie wiedzą, że kluczowy element złośliwego oprogramowania wykorzystanego w cyberataku został opracowany przez National Security Agency (NSA).

Od 2017 roku, kiedy NSA utraciła kontrolę nad narzędziem EternalBlue, stało się ono bronią wielu państwowych grup hakerskich, w tym z Korei Północnej, Rosji, a ostatnio również z Chin. Obecnie amerykańskie narzędzie hakerskie zostało wymierzone w samych Amerykanów.

Kampania cyberataków nie ogranicza się jedynie do Baltimore. Według specjalistów ds. cyberbezpieczeństwa działania hakerów, wykorzystujące EternalBlue, wymierzone są również w inne wrażliwe regiony i ich miasta – od Pensylwanii po Teksas. Cyberprzestępcy paraliżują samorządy lokalne oraz generują ogromne straty.

EternalBlue był jednym z najbardziej użytecznych narzędzi NSA. Jak informują anonimowi przedstawiciele Agencji, specjaliści pracowali przez prawie rok, aby znaleźć luki w oprogramowaniu Microsoftu i opracować kod, umożliwiający jego kierowanie. Z czasem nowa broń NSA stała się niezawodnym narzędziem wykorzystywanym w niezliczonych misjach wywiadowczych i antyterrorystycznych. „EternalBlue był dla Agencji tak cenny, że nigdy poważnie nie rozważano możliwości powiadomienia Microsoftu o odkrytych lukach” – wskazuje były pracownik NSA.

Cyberatak na Baltimore był klasycznym przykładem kampanii ransomware. Komputery zostały zablokowane, po czym wyświetlona została informacja o wymogu wpłaty 100 000 dolarów w Bitcoinach, aby odwrócić sytuację. Urzędnicy miejscy odmówili zapłaty okupu.

Jak wskazują specjaliści, bez EternalBlue szkody nie byłyby tak duże. Narzędzie wykorzystuje lukę w oprogramowaniu, która umożliwia hakerom szybsze rozprzestrzenianie szkodliwego elementu na większą skalę. „To niesamowite, że narzędzie wykorzystywane przez służby wywiadowcze jest obecnie publicznie dostępne i tak powszechnie używane” – stwierdził Vikram Thakur, dyrektor Symantec.

Hakerzy przy wyborze celów kierują się liczbą urządzeń w danej placówce, posiadających przestarzałe oprogramowanie. Microsoft, który śledzi korzystanie z EternalBlue, nie wymienia nazw miejscowości narażonych lub dotkniętych cyberatakiem. Jednak eksperci twierdzą, że kampania obejmuje m.in. Baltimore, Allentown i San Antonio.

„Nie można mieć nadziei, że gdy początkowa fala ataków się zakończy, cała kampania zniknie” – stwierdziła Jen Miller-Osborn, zastępca dyrektora w Palo Alto Networks. – „Spodziewamy się, że EternalBlue będzie używany prawie zawsze, ponieważ jeśli atakujący znajdą system, który nadal posiada luki, jest to bardzo przydatne narzędzie” – dodaje.

Michael S. Rogers, były dyrektor NSA podczas sugeruje, że Agencji nie należy obwiniać za całą sytuację. „Jeśli Toyota produkuje pickupy i ktoś bierze takiego pickupa, umieszcza na nim bombę, następnie wjeżdża w tłum ludzi, detonując ładunek – czy to wina Toyoty?” – tłumaczy Michael Rogers. – „NSA opracowała narzędzie, które nigdy nie zostało zaprojektowane do tego, co obecnie ma miejsce”.

Słowa dyrektora NSA wywołały falę sprzeciwu. Wielu ekspertów krytycznie odniosło się do tłumaczenia. „Całkowicie się nie zgadzam” – zaznaczył Tom Burt, wiceprezes w Microsoft. – „To narzędzie zostało opracowywane i utrzymywane w tajemnicy przez państwo w celu wykorzystania go do szpiegowania. Z natury jest niebezpieczne”. Bezpośrednio odnosząc się do słów dyrektora NSA Tom Burt zaznaczył – „Kiedy ktoś je bierze (przyp. red. EternalBlue), nie przypina do niego bomby. To już bomba”.