Globalny cyberatak

14 maja 2017
Od piątku 12 maja co najmniej 100 tysięcy komputerów w co najmniej 99 krajach zostały zaatakowane wirusem, który szyfruje zawartość ich plików i domaga się 300 USD okupu za ich odblokowanie. Płatność oczywiście w Bitcoin. Celem ataku są przede wszystkim Rosja, USA, Europa, Ameryka Płd, Indie, Japonia, Filipiny i Chiny. W zasadzie atak nie ominął żadnego kontynentu. Jak na razie (13 maja 2017) najmniej ucierpiały Afryka, Kanada i Australia. Najbardziej – Rosja.

Wirus o nazwie WannaCry [Chcę płakać] nazywany też WannaCrypt [Chcę zaszyfrować] atakuje głównie systemy sieci połączonych ze sobą, więc jego ofiarami są przede wszystkim zsieciowane instytucje na całym świecie. Począwszy od szpitali (w Wlk. Brytanii praktycznie sparaliżowany jest cały system szpitalnego leczenia), poprzez systemy zarządzające komunikacją (niemieckie koleje państwowe), skończywszy na tysiącach różnego rodzaju firm i instytucji (np. FedEx, hiszpańska sieć telekomunikacyjna Telefónica, portugalski Telecom, rosyjski MegaFon) – wirus zablokował możliwość użytkowania systemów komputerowych.

W zasadzie większość obserwatorów rozwijającego się wciąż cyberataku jest zgodna w swojej opinii, że zastosowane ransomware (ransom to okup po angielsku) pochodzi z archiwum National Security Agency (NSA) i że właśnie zastosowano narzędzia o których Wikileaks niedawno pisało, że są dostępne w sieci na tzw. czarnym rynku. Przyznają to nawet tak zeszmacone źródła, jak „Politico” czy też „New York Times”. O skandalu związanym z utratą kontroli nad nielegalnie stworzonym arsenałem cybernarzędzi przez rząd USA traktowała ostatnio cała seria przecieków Wilikeaks o nazwie Vault 7.

Edward Snowden zauważył, że NSA miało obowiązek przestrzec

wszystkie zagrożone systemy komputerowe i przygotować dla nich oprogramowanie ochronne – zwłaszcza od momentu, gdy było wiadomo, że NSA utraciło kontrolę nad tym nielegalnym arsenałem cybernarzędzi. NSA oczywiście takiego ruchu nie wykonało. I możemy być pewni, że nie poniesie z tego tytuły żadnej odpowiedzialności. Jak i cały Deep State, który za tą przestępczą działalnością różnych rządowych amerykańskich agencji stoi.

Tym razem amerykańska propaganda nie będzie mogła tradycyjnie zrzucić winy za atak na Rosję, albowiem Rosja jak na razie jest jedną z głównych ofiarą ataku. Z ciekawostek: podobno użytkownicy Windows 10 – systemu, który jest pierwszym całościowo inwigilującym systemem operacyjnym na usługach amerykańskich rządowych agend – nie są zagrożeni atakiem WannaCry.

Microsoft opublikował łatkę dla starych systemów, które są najbardziej podatne na atak (Windows 8, XP, Vista) i jest ona teoretycznie dostępne na stronie Microsoft. Piszę „teoretycznie" albowiem być może na skutek przeciążenia strony albo też z innych przyczyn mnie się nie udało takiej łatki z tej strony ściągnąć. Głównym kanałem zakażania komputerów jest poczta mailowa i spam. Tak więc uważaj na maile, które znajdziesz w swojej skrzynce. Jeżeli zakażeniu ulegnie zsieciowany komputer, wirus już dalej się dystrybuuje poza wszelką kontrolą po całej sieci.

Autorstwo: Andreas
Na podstawie: RT.com i inne strony
Źródło: EfektSetnejMalpy.pl