EKSPERT: ATAK RANSOMWARE MOŻLIWY DZIĘKI NSA

Do ataku ransomware, który przetoczył się przez systemy na całym świecie wykorzystano narzędzia wykradzione NSA – mówi konsultant cyberbezpieczeństwa i prywatności dr Łukasz Olejnik. Uzbrojono je i przekształcono w automat do cyberataków.

Ransmoware to złośliwe oprogramowanie, za pomocą którego hakerzy żądają okupu w zamian za odblokowanie dostępu do sieci teleinformatycznych lub komputerów. Niezależny badacz zwrócił uwagę, że sprawa dotyczy prawie 100 państw, a skutki ataku odczuła m.in. brytyjska publiczna służba zdrowia NHS, czy największy hiszpański telekom - Telefonica. Zdaniem Olejnika piątkowy atak świadczy o tym, że "problem jest globalny i polityczny".

> *Ten ransomware jest szczególnie ciekawy, bo wykorzystuje narzędzia - zwane ETERNALBLUE - wykradzione amerykańskiej NSA (Agencja Bezpieczeństwa Narodowego), które uzbrojono i przekształcono w automat do cyberataków" - podkreślił konsultant cyberbezpieczeństwa i prywatności. Gdy te narzędzia wyciekły i zostały upublicznione, wśród specjalistów spodziewano się tego, jako najgorszego scenariusza. Już wykorzystuje się ten fakt do krytyki wywiadów elektronicznych przechowujących tego typu narzędzia będące - jak widać - zagrożeniem dla całego świata. Problematyka ta jest jednak znacznie szersza i skomplikowana.*
>
> *dr Łukasz Olejnik, konsultant cyberbezpieczeństwa i prywatności*

W ocenie Olejnika piątkowy atak ransomware "już jest największym w historii". Przypomniał dawne sławne cyberataki robaków sieciowych Conficker - a wcześniej Nimda". Z drugiej strony – jak mówi Olejnik - mimo skali ataku, operatorzy tego ransomware jak dotychczas nie zarobili wiele, ok. 13 tys. dolarów; do soboty rano jedynie ok. 50 ofiar zdecydowało się zapłacić okup. Mimo wielkiego zasięgu ataku - ransomware bijący w newralgiczne elementy społeczne i towarzysząca temu sława to jednak coś, co niekoniecznie pomaga właścicielom tego złośliwego oprogramowania w maksymalizacji zysku.

Czytaj też: Czarny piątek. Ransomware, czyli wymuszenie okupu coraz popularniejsze

Ekspert zwrócił też uwagę, że ostatecznie udało się znaleźć mechanizm "wyłączający" te złośliwe oprogramowanie, choć "stosunkowo łatwo przetworzyć jego kod", dlatego nadal istnieje ryzyko

powrotu podobnych ataków. Jak jednocześnie dodał, tego ataku nie można było uniknąć.

> *Dwa miesiące temu Microsoft wydał poprawki bezpieczeństwa (MS17-010) na podatność stosowaną w ataku. Wystarczyło zatem zaktualizować systemy. Na przykładzie tego ataku widać doskonale, jak złożonym problemem jest cyberbezpieczeństwo, i jaki wpływ na nie ma pewnego rodzaju bezwład cechujący duże organizacje - korporacje, instytucje publiczne. Wbrew temu, czego życzy sobie szefowa MSW Wielkiej Brytanii Amber Rudd, całe zagadnienie jest dużo głębsze, niż sam fakt instalacji poprawek oprogramowania.*
>
> *dr Łukasz Olejnik, konsultant cyberbezpieczeństwa i prywatności*

Podsumowując ekspert ds. cyberbezpieczeństwa podkreślił, że wydarzenia z piątku pokazują, że "problem dotyczy strategii cyberbezpieczeństwa na poziomie organizacji jak i państwa".