**WCry - ten atak może się powtórzyć. Check Point informuje o zagrożeniu**

**Zmasowany, ogólnoświatowy atak złośliwego oprogramowania typu ransomware, którego ofiarą padły komputery z systemem operacyjnym Windows w ok. 100 krajach, w sobotę został praktycznie powstrzymany. Może jednak dojść do kolejnych ataków ransomware – ostrzega Check Point.**

Powstrzymanie ataku jest wynikiem wykrycia przez eksperta IT tzw. wyłącznika awaryjnego w oprogramowaniu, wymuszającym okup w bitcoinach za odblokowanie plików, zaszyfrowanych przez hakerów w zaatakowanych komputerach. Informatyk zorientował się, że to złośliwe oprogramowanie (WannaCrypt, WanaCrypt lub Wcry) atakuje urządzenia z systemem operacyjnym Windows i używa luki odkrytej przez Microsoft. Ta została załatana w marcu bieżącego roku, ale jak widać, wciąż wiele komputerów nie zostało zaktualizowanych, co pozwala na zainfekowanie maszyn.

Kampania objęła m.in. instytucje państwowe w Wielkiej Brytanii, gdzie ofiarą stała się Narodowa Instytucja Ochrony Zdrowia (NHS) . Atak doprowadził‚ do krachu systemów komputerowych i co za tym idzie, dostarczania opieki medycznej. Wiele planowanych operacji na razie zostało przełożonych.

Skutki ataku odczuły firmy w Rosji, Turcji, Niemczech, Indonezji, Wietnamie, Japonii, Hiszpanii. W Hiszpanii ofiarami ataku padĹ‚ potentat telekomunikacji Telefonica oraz bank Santander. Na całym świecie jego ofiarą padają różne organizacje, np. uniwersytety, usługi telekomunikacyjne, banki oraz szpitale.

*- To relatywnie nowa odmiana ransomware, po raz pierwszy wykryta w lutym 2017 roku, a jej najnowsza wersja ujawniła się w dniu 11 maja 2017. Niebezpieczeństwo tkwi w bardzo szybkim procesie rozprzestrzeniania się tego wirusa w sieciach organizacji i korporacji w Europie i Azji. To pokazuje prawdziwe oblicze i problem jaki niesie ze sobą ransomware* - podkreśla Aatish Pattni, szef oddziału prewencji w firmie Check Point, Północna Europa.

*- Atak ten uświadamia światu, że wszystkie firmy i organizacje muszą… bardziej szczegółowo podchodzić do kwestii skanowania i filtrowania niebezpiecznych plików, które trafiają do systemów sieciowych. Najistotniejszym elementem jednak jest proces szkoleń pracowniczych i ochrony przenośnych urządzeń używanych do korespondencji służbowej* - dodaje przedstawiciel Check Point.