Złośliwe oprogramowanie 2017 - Ransomware

WannaCry (znany również jako **WannaCrypt** lub **WanaCrypt0r 2.0**) – złośliwe oprogramowanie typu **ransomware**. Duża fala cyberataków za pomocą tego oprogramowania miała miejsce w maju 2017, kiedy to zarażonych zostało ponad 300 tys. komputerów w 99 krajach. Przestępcy żądali zapłaty w 28 językach (w tym polskim). Według danych Europolu był to największy atak tego rodzaju w ostatnim czasie.

W ataku ucierpiała Telefónica i kilka innych dużych przedsiębiorstw w Hiszpanii, a także części brytyjskiej narodowej służby zdrowia, Fedex oraz Deutsche Bahn. Media donosiły także, że inne cele w co najmniej 99 krajach również zostały zaatakowane w tym samym czasie. W Rosji zainfekowanych zostało ponad 1000 komputerów w ministerstwie spraw wewnętrznych, agencji zarządzania sytuacjami kryzysowymi (EMERCOM) oraz w przedsiębiorstwie telekomunikacyjnym MegaFon. Do 17 maja łączny okup jaki dostali hakerzy wynosił ponad 79 tys. USD.

WannaCry wykorzystuje *exploit* o nazwie *EternalBlue*, który rzekomo został zaprojektowany w amerykańskiej agencji bezpieczeństwa narodowego w celu atakowania komputerów z systemem Windows. Nie ma pewności jak WannaCry infekuje daną sieć, jednak po zainfekowaniu jednego komputera, infekuje pozostałe komputery w sieci lokalnej za pomocą starej wersji protokołu SMB.

Struktura kodu WannaCry przypomina te z wcześniejszych ataków północnokoreańskiej grupy Lazarus.

Łatka do tej luki bezpieczeństwa została wydana przez Microsoft już 14 marca 2017. Jednak wiele komputerów pozostało narażonych ze względu na opóźnienia w instalacji aktualizacji zabezpieczeń. Użytkownicy systemu Windows XP, który nie jest wspierany przez Microsoft od kwietnia 2014, nie otrzymali marcowej aktualizacji. Jednak po serii ataków WannaCry, 12 maja 2017, producent zdecydował się opublikować poprawkę dla wszystkich użytkowników Windows XP.

12 maja 2017 r. Marcus Hutchins z Kryptos Logic znalazł próbkę kodu wirusa i ustalił, że oprogramowanie łączyło się z niezarejestrowaną domeną. Hutchins postanowił zarejestrować domenę na siebie, co zatrzymało infekowanie kolejnych komputerów.

https://pl.wikipedia.org/wiki/WannaCry

Petya

Microsoft opublikował raport po wielkim ataku ransomware **Petya** w czerwcu 2017 r. Według giganta z Redmond do infekcji nie doszło na tak wielką skalę, jak w przypadku WannaCry. Użytkownicy systemu Windows 10 nie byli ofiarami nowego ataku. Petya największe spustoszenie dokonała na komputerach z nieaktualnym Windows 7.

Microsoft przeanalizował atak ransomware o nazwie Petya. Z informacji przekazanych przez giganta z Redmond wynika, że wszystko zaczęło się od infekcji komputerów na Ukrainie i to właśnie tam największe szkody wyrządził nowy wirus. Microsoft szacuje, że **około 70% wszystkich zainfekowanych maszyn pochodziło z Ukrainy**.

Petya nie zdołała wyrządzić tak wielkich szkód, jak to miało miejsce w przypadku WannaCry. Według Microsoft **zainfekowano „tylko" około 20 tysięcy komputerów.** Najczęściej były to maszyny pracujące pod kontrolą systemu Windows 7.

Warto dodać, że Microsoft załatał już lukę wykorzystywaną przez Petya czy WannaCry w marcu tego roku. Do infekcji dochodziło więc na maszynach, które nie były cyklicznie aktualizowane. Gigant z Redmond zachęca więc do uaktualniania oprogramowania własnych komputerów, co często może ochronić przed skutkami tego typu ataków.

Microsoft zauważa również, że doczekaliśmy się czasów, gdzie ataki z wykorzystaniem złośliwego oprogramowania na masową skalę są coraz skuteczniejsze. Trend ten zaczyna się umacniać, co jest niepokojące. Cyberprzestępcy sięgają po coraz bardziej zaawansowane metody, które są w stanie doprowadzić do szkód na wielką skalę.

http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2017/26/microsoft-petya-wyrzadzila-mniej-szkod-niz-wannacry-ofiarami-glownie-komputery-z-windows-7.aspx