Cyberdefence 24

26.10.2017

BAD RABBIT POWIĄZANY Z NOTPETYA

Wirus Bad Rabbit mający na celu wyłudzenie okupu wykazuje wyraźne powiązania ze szkodliwym programem ExPetr - twierdzą eksperci. Wszystkie wykryte dotychczas ataki miały miejsce we wtorek. Celem padły komputery m.in. w Rosji, Turcji, Niemczech i na Ukrainie.

Eksperci monitorujący aktywność nowego wirusa porównują Bad Rabbit do wcześniejszych ataków szyfrujących komputery - WannaCry i ExPetr (inaczej Petya lub NotPetya), wykorzystanych na szeroką skalę w atakach hakerskich mających na celu wyłudzanie okupu w czerwcu 2017.

> *Możemy zaobserwować pewne podobieństwa do poprzedniego ataku (Not)Petya, ponieważ Bad Rabbit próbuje rozprzestrzeniać się dalej z wykorzystaniem niektórych elementów znanych z poprzedniego incydentu*
>
> *Marek Krauze - ekspert ds. cyberbezpieczeństwa w Trend Micro*

Analiza przeprowadzona przez zespół Kaspersky Lab wykazała podobieństwa w kodach źródłowych, mechanizmie szyfrującym dane dla okupu, a także w domenach wykorzystywanych przez cyberprzestępców do koordynowania ataków z zastosowaniem Bad Rabbit i ExPetr. Podobnie jak ten ostatni, Bad Rabbit próbuje uzyskiwać dane uwierzytelniające przy użyciu usługi WMIC systemu Windows. Dotychczas nie udało się jednak ustalić, czy Bad Rabbit również korzysta z narzędzi EternalBlue oraz EternalRomance wykorzystujących luki w zabezpieczeniach systemu.

Czytaj więcej: Ransomware Bad Rabbit uderza w Rosję, Ukrainę i inne państwa

> *Jedną z początkowych metod infekcji były tak zwane wodopoje (waterholes) – strony przejęte przez przestępców, którzy wgrali tam instalator popularnego oprogramowania zainfekowanego szkodliwym kodem. Na taki atak może być narażony praktycznie każdy użytkownik systemów komputerowych*
>
> *Marek Krauze - ekspert ds. cyberbezpieczeństwa w Trend Micro*

Złośliwe oprogramowanie miało rozprzestrzeniać się przez zhakowane wcześniej strony rosyjskich mediów, takich jak agencja informacyjna Interfax czy petersburski portal Fontanka. Bad Rabbit zainfekował ok. 200 komputerów, jednak od tego czasu nie zarejestrowano nowych ataków. Cyberatakiem dotknięte zostały m.in. obiekty infrastruktury, takie jak np. lotnisko w Odessie czy metro w Kijowie na Ukrainie. Choć atak dotarł również do Turcji, Niemiec i Polski, większość firm poszkodowanych w wyniku działania wirusa ma się znajdować w Rosji. Stojący za złośliwym oprogramowaniem cyberprzestępcy mieli przygotowywać atak co najmniej od lipca 2017.

Hakerzy stojący za wirusem Bad Rabbit szyfrują komputery za pomocą złośliwego oprogramowania i domagają się 0,05 Bitcoina (około 288 dolarów) okupu za odszyfrowanie. Według komunikatu, który wyświetla się na ekranach zainfekowanych wirusem Bad Rabbit komputerów, wysokość okupu żądanego przez hakerów niebawem wzrośnie.

Eksperci w dziedzinie cyberbezpieczeństwa odradzają ofiarom hakerów płacenie okupu, bo - jak wskazują - zachęca to przestępców do dalszej aktywności. Nie ma też gwarancji, że uregulowanie okupu faktycznie będzie prowadziło do odblokowania dostępu do urządzenia. Aby uniknąć zarażenia wirusem należy wystrzegać się uruchamiania nieznanych, podejrzanych załączników i klikania w niesprawdzone linki w poczcie. Atak od początku jest wykrywany m.in. przez systemy TrendX i Deep Discovery wykorzystujące uczenie maszynowe.