Cyberdefence 24

aut. Adam Lelonek 25.10.2017

RANSOMWARE BAD RABBIT UDERZA W ROSJĘ, UKRAINĘ I INNE PAŃSTWA

Nowe oprogramowanie wymuszające okup o nazwie „Bad Rabbit", przypominające wcześniejsze ransomware WannaCry czy uznawanego za symulację działania ransomware NotPetya, zostało zidentyfikowane głównie w Rosji i na Ukrainie, ale również w Niemczech czy Japonii. Nowy atak cybernetyczny stwarza zagrożenie dla systemów w całej Europie. Trwał on od rana do ok. południa 24 października, lecz kolejne ofiary są wciąż identyfikowane.

Jak twierdzi firma ESET proporcje wykrywania aktywności związanych z atakiem są następujące: w Rosji było 65% przypadków, na Ukrainie – 12,2%, w Bułgarii – 10,2%, Turcji – 6,4%, Japonii – 3,8% i innych krajach, w tym Niemczech – 2,4%. Na Ukrainie zaatakowane zostało lotnisko w Odessie i kijowskie metro. Wśród ofiar znajduje się również strona agencji Interfax i Fontanka.ru. Jest to część tego samego cyberataku, skierowanego głównie wobec sieci firmowych. Wśród zaatakowanych stron najwięcej jest tych należących do mediów. Łącznie na chwilę obecną mówi się o 200 dotkniętych podmiotach. Eksperci z firmy ESET zwracają uwagę, że wszystkie podmioty zostały zaatakowane jednocześnie.

Strona ukraińska twierdzi, że nie ma mowy o globalnym ataku cybernetycznym oraz że Służba Bezpieczeństwa Ukrainy już 12 października informowała o możliwych działaniach hakerów skierowanych przeciwko podmiotom państwowym i prywatnym, przypominających wcześniejsze schematy. Zwracano też uwagę, że jedną z metod mogą być fałszywe aktualizacje popularnych programów.

Rosyjska firma zajmująca się cyberbezpieczeństwem Group-IB twierdzi, że praca wielu rosyjskich firm została całkowicie sparaliżowana z powodu zaszyfrowania stanowisk pracy i serwerów. Firma Kaspersky Lab twierdzi, iż Rosja jest największą ofiarą tego ataku. Firma ESET informuje, że złośliwe oprogramowanie użyte do szyfrowania to Diskcoder.D – nowy wariant ransomware znanego jako Petya. Wykorzystuje on narzędzie Mimikatz to pozyskania danych z zainfekowanych systemów.

Płatność, której żądają hakerzy, to 0,05 bitoina, czyli ok. 280 dolarów. Zgodnie z komunikatami pojawiającymi się na przejętych komputerach cena ta będzie wzrastać. Eksperci z obu stron oceanu odradzają płacenie okupu, gdyż nie ma żadnej gwarancji, iż dane zostaną przywrócone. Do tego płacenie hakerom tylko zachęca ich do dalszych ataków.

Wiele programów antywirusowych jeszcze nie radzi sobie z detekcją nowego złośliwego oprogramowania. Przedstawiciele firmy ESET twierdzą, iż Bad Rabbit był dystrybuowany przez nieprawdziwą aktualizację Adobe Flash. Podobnie uważają przedstawiciele Kaspersky Lab, którzy aktywnie komentują całe zajście. W Rosji rozprzestrzenianie odbywało się przez zhakowane strony internetowe prawdziwych mediów. Z tej strony pobierana był „dropper" ze złośliwym oprogramowaniem, udającym aktualizację lub instalatora Adobe Flash. Atak następował, kiedy użytkownik klikał w komunikat o dostępnej nowej aktualizacji, a następnie pobrał i zainstalował plik „install_flash_player.exe", po uprzednim zatwierdzeniu dodatkowych uprawnień administracyjnych.

Hakerzy zwrócili uwagę analityków przez wpisywanie do kodu złośliwego oprogramowania nazw dwóch smoków z serialu „Gra o tron": Drogon i Rhaegal oraz innych postaci. Już teraz wiele mediów określa ich jako miłośników serialu.