Cyberdefence 24

aut. Tomasz Fastyn 09.08.2016

PO BLISKO 5 LATACH BADAŃ ZBADANO WIRUSA SAURON

W dwóch osobnych raportach opublikowanych przez firmy Kaspersky Lab oraz Symantec, wirus obecny w przestrzeni sieciowej od 2011 roku został nareszcie rozpisany oraz zbadany w odpowiedni sposób. Powód dla którego dopiero teraz zbadano wirusa atakującego sieci rządowe to wysoki poziom zabezpieczeń przed wtargnięcie do jego źródeł kodu. Według niektórych ekspertów cyberbezpieczeństwa za wirusem mogą stać nawet agencje rządowe.

Project Sauron to grupa, która odpowiada za stworzenie oraz udostępnienie wirusa, który na przestrzeni ostatnich 5 lat spowodował infekcję w sieciach rządowych na terenie Belgii, Szwecji, Rosji oraz Chin - jak podaję firma Symatec w swoim raporcie. Problem dla którego tak długo zajęło specjalistom ds. wirusów oraz bezpieczeństwa informatycznego zbadanie tego programu, może polegać na opisanym w raporcie Kaspersky Lab mechanizmie obronny – rozbiciu samego wirusa na 50 modułów dopasowanych do atakowanych sieci. Hakerzy najwidoczniej byli bardzo dobrze poinformowani o składnikach atakowanej infrastruktury, nawet na temat używanych w agencjach rządowych antywirusów i oprogramowania. Wstrzyknięcie wirusa do sieci w jednej z faz polegało na modyfikacji oprogramowania występującego na komputerze użytkownika, podmieniano potem skrypty aplikacji dostarczając jednocześnie plik umożliwiający pobranie samego złośliwego oprogramowania.

Sauron od tej porty kojarzony przez system z bezpieczną i zaufaną aplikacją mógł rozpocząć działanie. Według raportu Kaspersky Lab miało to być oprogramowanie używane na co dzień, takie jak tworzone przez VMware, Hewlett-Packard, Microsoft, Symantec czy nawet Kaspersky Lab.

Do tej porty zidentyfikowano 30 ofiar samego wirusa, który według ekspertów z obu firm jest z dużą dozą prawdopodobieństwa stworzony na potrzeby lub z finansową pomocą agencji rządowych. Ma to wynikać z używania zaawansowanych mechanizmów oraz modułów dostosowujących wirusa do ataków na nowe cele, na to według ekspertów może sobie pozwolić tylko niewiele grup hakerskich. To też spowodowało, że ataki były początkowo brane jako wykonywane za pomocą nowego złośliwego oprogramowania. Strider, nazwany tak początkowo przez firmę Symantec wirus, zyskał przydomek Sauron, z powodu występowania tej nazwy w odkrytym nie tak dawno kodzie.

Oprócz wymienionych krajów jak Rosja, w której odnaleziono co najmniej 30 zarażonych komputerów, w tym cztery należące do prywatnych osób, cele pojawiały się także Iranie oraz Rwandzie. Jaki kraj z jakiego rejonu świata stoi za produkcją tego akurat wirusa, nie wiemy i znając ostrożność służby wywiadowczych raczej nie poznamy tej tajemnicy. Można tylko gdybać kto mógłby stać za atakiem na taką skalę. Remsec bo tak nazywa się sam moduł działający, który został dostarczony na komputery, które wybrali hakerzy jest mało znany nawet ekspertom z laboratoriów Symantec oraz Kaspersky Lab. Do tej pory udało się jedynie ustalić, że będąc w systemie wirus działa wyłącznie z poziomu pamięci komputera, stamtąd może np. za pomocą keyloggera sczytywać wprowadzane znaki za pomocą klawiatury komputera.

Oprócz tego hakerzy stworzyli wirusa tak, aby dokładnie skanował wszelkie komponenty szyfrowanej komunikacji, klucze szyfrujące, pliki konfiguracyjne czy nawet lokalizację poszczególnych serwerów wykorzystywane do tej komunikacji.

Język oprogramowania użyty przez hakerów (Lua) do stworzenia oprogramowania nie jest popularny, do tej pory został jedynie użyty przy innych wirusach sponsorowanych przez agencje rządowe, chodzi o kampanie Flame oraz Animal Farm. Flame podobnie jak Stuxnet został wprost nazwany przez ekspertów cyberbezpieczeństwa jako twór osób ściśle powiązanych z NSA oraz izraelskim wywiadem. Stąd najprawdopodobniej pojawiają się wnioski ekspertów, że ze względu na użyty język oprogramowania oraz cele ataków umiejscowione w tych a nie innych krajach świata oraz poziom zaawansowania wirusa można śmiało powiedzieć, że jest on finansowany przez służby. Wywiad stojący za produkcją wirusa, nie należy raczej do tych o małym znaczeniu geopolitycznym.

Czytaj też: Rywalizacja pomiędzy hakerami – twórcy ransomware ujawnili prywatne klucze przeciwnika