Atakuje Windowsa, by zainfekować Linuksa

23 lutego 2017

Eksperci z firmy Kaspersky ostrzegają, że skutki ataku złośliwego kodu Mirai – który bierze na cel urządzenia z Linuksem i tworzy z nich botnet – mogą być groźniejsze, niż się początkowo wydawało. Specjaliści odkryli bowiem złośliwy kod na Windowsa, który najpierw infekuje pecety z systemem z Redmond, a następnie korzysta z nich by wyszukać urządzenia z Linuksem i zainfekować je kodem Mirai.

Zdaniem pracowników Kaspersky'ego twórca kodu atakującego Windowsa ma większą wiedzę i umiejętności niż twórca Mirai. Wskazuje to, że osoba bądź osoby stojące za złośliwym kodem dla Windowsa mają własne plany dotyczące wykorzystania linuksowego botnetu stworzonego przez Mirai. „Bazujący na Windowsie kod rozprzestrzeniający Mirai jest bardziej złożony i solidny niż kod Mirai, jednak większość użytych w nim technik i funkcji liczy sobie kilka lat" – stwierdzają eksperci.

Na szczęście sposób działania nowego kodu jest ograniczony. „Może on zarazić kodem Mirai tylko te linuksowe urządzenia typu internet-of-things, które sa podatne na atak brute force za pomocą Telnetu" – stwierdzają pracownicy Kaspersky'ego. Wszystko wskazuje na to, że twórca kodu na Windows pochodzi z Chin. Język użyty w kodzie, fakt, iż został on skompilowany na chińskiej wersji systemu, że serwery go hostujące znajdują się na Tajwanie oraz fakt, iż kod został podpisany certyfikatami skradzionymi chińskim firmom wskazuje na jego pochodzenie z Państwa Środka.

W bieżącym roku windowsowy kod zarażający Mirai zaatakował około 500 systemów. Nie jest to dużo, ale warto zauważyć, że ofiary pochodzą przede wszystkim z państw rozwijających się,

które mocno inwestują w IoT. Wśród ofiar nowego kodu są systemy z Indii, Wietnamu, Arabii Saudyjskiej, Chin, Iranu, Brazylii, Maroka, Turcji, Malawi, Mołdowy, Rosji, Egiptu, Kolumbii czy Bangladeszu. Eksperci obawiają się, że to może być dopiero początek, a wkrótce do rozprzestrzeniania Mirai za pomocą Windows może wziąć się ktoś o naprawdę dużych umiejętnościach i zasobach.

Tymczasem znany bloger Brian Klebs uważa, że twórcą kodu Mirai jest amerykański student.

Autorstwo: Mariusz Błoński
Na podstawie: Computing.co.uk
Źródło: KopalniaWiedzy.pl