**Bitdefender informuje, że Pushdo Botnet zainfekował ponad 76,000 maszyn**

**Zainfekowanych sieci komputerowych przez Pushdo jest znacznie więcej, niż przewidywano**

początkowo. Firma Bitdefender wykazała, że ponad 76,000 maszyn podłączonych do domen zostało

zainfekowanych, jak wykazuje informacja opublikowana przez softpedia.com w dniu 21 lipca 2014.

W ostatnim tygodniu lipca Bitdefender umieścił informację na temat nowej wersji Pushido

malware, stwierdzając, że nowy szczep pojawił się wraz z nowym DGA (algorytm generowania

domeny) i zawierał odmienne klucze prywatne i publiczne dla zaszyfrowanego połączenia z centrum

zarządzania serwerem (C2).

Bitdefender niedawno informował, że coraz więcej komputerów zostało zainfekowanych

przez złośliwe oprogramowanie. Do poniedziałku 21 lipca 2014 zaobserwowano 784000 wywołań,

które posiadały 76,433 unikalne adresy IP.

Bitdefender znalazł 2,336 adresów IP połączonych z systemem gdzie zagrożenia czekały na

instrukcje w odstępach czasowych mniejszych niż 3 godziny.

Dane zebrane przez Bitdefender wykazały, że najwięcej infekcji zostało zauważone w Indiach

(4215), Wietnamie (3637), Stanach Zjednoczonych (2153), Argentynie (2075), Turcji (2045), Meksyku

(1811), Indonezji (1755), Iranie (1561 ), Włoszech (1393) i Tajlandii (1107). Setki infekcji wykryto na

Tajwanie, na Filipinach, w Egipcie, Brazylii, Peru, Francji, Malezji, Rosji, RPA, Kolumbii, Pakistanie,

Polsce, Chinach, Hiszpanii, Korei Południowej, Niemiec, Wielkiej Brytanii i Japonii.

Bitdefender poinformował, że zgodnie z najnowszymi obliczeniami, wpływ botnetu wciąż jest

najsilniejszy w Azji, Indie (21768) są najbardziej dotknięte, zaraz za nimi jest Wietnam (20043),

Islamska Republika Iranu (9787), Stany Zjednoczone (9001 ), Turcja (8865), Indonezja (8240),

Tajlandia (8062), Argentyna (6212), Peru (5828) i Meksyk (5447).

Bitdefender.com pod koniec lipca opublikował informację z cytatem wypowiedzi Doina

Cosovan badacza z firmy Bitdefender „Ogólnie uważamy, że jest to dość powszechny botnet, posiada

umiejętność dowodzenia i kontroli systemu co symbolizuje bardzo szybkie przeniesienie się na

używanie nowego DGA.”