F-SECURE: ROSJA I NIEMCY GŁÓWNYMI ŹRÓDŁAMI CYBERATAKÓW NA POLSKĘ

Od kwietnia do września 2017 z Rosji podjęto ponad 2,5 miliona prób cyberataków na Polskę. Na drugim miejscu jako źródło napaści komputerowych znalazły się Niemcy, choć z dziesięciokrotnie mniejszym wynikiem - wynika z raportu opracowanego przez F-Secure.

Informacje o atakach komputerowych zostały uzyskane przez działająca w branży cyberbezpieczeństwa firmę F-Secure dzięki autorskiej sieci tzw. honeypotów, czyli udających łatwy cel serwerów stanowiących przynętę dla hakerów. Dzięki obserwacji prowadzonych na nie ataków możliwe jest pozyskanie cennych danych przydatnych w opracowywaniu nowych metod walki z cyberzagrożeniami.

W analizowanych sześciu miesiącach najwięcej ataków na cele w Polsce prowadzono z Rosji - średnio tamtejsi hakerzy podejmowali ponad 14,5 tys. prób ataków dziennie. "Rosyjskie adresy IP najczęściej próbowały uzyskać nieautoryzowany dostęp do urządzeń (protokół SSH), ale równie duży był udział połączeń na port SMTP, co wskazuje na aktywność w rozsyłaniu tzw. spamu" – mówi lider Centrum Cyberbezpieczeństwa F-Secure w Poznaniu Leszek Tasiemski.

"To jedyny kraj o tego typu profilu i wygląda na to, że to z terytorium Rosji operują gangi czerpiące zyski z tego procederu" - dodaje Tasiemski. Jego zdaniem winą za to można obarczać słabo zabezpieczoną infrastrukturę i niską skuteczność rosyjskich organów ścigania w tropieniu spamerów.

Drugie miejsce jeśli chodzi o podejrzany ruch sieciowy w kierunku Polski stanowią adresy IP przynależne do Niemiec. W minionym półroczu z ich strony wyszło ponad 250 tys. prób ataków - średnio 1,4 tys. dziennie.

"W przypadku ataków z Niemiec, jak i Francji oraz USA uwagę zwraca duży dział połączeń na port telefonii internetowej (SIP). Może mieć to związek z próbą kradzieży informacji (podsłuchy) lub spamu realizowanego drogą telefoniczną. Polega to na wykorzystywaniu skradzionej infrastruktury do wykonywania połączeń reklamowych na koszt skutecznie zaatakowanego podmiotu" – komentuje Tasiemski.

Trzecim krajem, z którego najczęściej atakowano Polskę okazały się Chiny, które od kwietnia do września br. przeprowadziły 183 tys. prób cyberataków(ok. 1 tys. ataków dziennie). Niemal na równi z Chinami znalazły się Stany Zjednoczone oraz Francja.

"Wśród zebranych danych wyróżniają się te dotyczące cyberataków z Chin. Większość działań dotyczy prób nawiązania połączenia z popularnymi bazami danych, zarówno MSSQL jak i MySQL. To wskazuje na nastawienie atakujących głównie na kradzież danych oraz szpiegostwo przemysłowe" – tłumaczy Tasiemski.

Dzięki sieci honeypot możliwe było opracowanie mapy najczęstszego występowania ataków w Polsce – według danych F-Secure są to Warszawa, Poznań, Kraków, Gdańsk i Katowice. Największe zagęszczenie wynika z dużej liczby użytkowników aglomeracji, a co za tym idzie również urządzeń. W dużych miastach znajdują się też węzły komunikacyjne dostawców usług internetowych, w związku z czym ruch sieciowy w tych miejscach jest bardziej intensywny.

"Liczba obserwowanych przez nas zdarzeń nie rośnie w zastraszającym tempie, niemniej widoczne są zmiany struktury ataków. Globalnie widzimy coraz większy udział ataków na porty związane z internetem rzeczy, co potwierdza konieczność zwrócenia uwagi na zabezpieczenia naszych «sprytnych» urządzeń codziennego użytku" - komentuje Tasiemski.

"Interesujące są też różnice między poszczególnymi krajami, ponieważ wskazują na pewien stopień specjalizacji operujących z ich terytorium hakerów. Należy pamiętać, że geografia w internecie jest rzeczą ulotną. Źródło to ostatni «przystanek», którego atakujący użył, i nie jest to jednoznaczne z jego fizycznym położeniem. Możliwe, że haker z Polski używa serwera w Rosji, żeby zaatakować cel w Brazylii" – podsumowuje przedstawiciel F-Secure.

pap