**Rozwijający się Internet rzeczy (IoT) coraz bardziej atrakcyjnym celem ataków cybernetycznych**

**Wzrostowi wykorzystania w gospodarstwach domowych sprzętu, który podłączany jest do sieci, towarzyszy gwałtownie rosnąca fala ataków, wykorzystujących słabe zabezpieczenia urządzeń internetu rzeczy. Mogą to być urządzenia AGD, routery, kamery internetowe, termostaty lub drukarki – charakter tych urządzeń nie ma dla cyberprzestępców znaczenia, byle by tylko były łatwe do naruszenia i odpowiadały celowi, z jakim włączane są do botnetu. Raport ogłoszony przez SonicWall ujawnia, że w 2017 r. przestępcy cybernetyczni mocno angażowali się w ataki na internet rzeczy (IoT), przeprowadzając ich nie mniej niż 10,3 miliona. W następnym roku aktywność na tym polu wzrosła jeszcze trzykrotnie, osiągając liczbę 32,7 miliona.**

Nie ma się czemu dziwić. W latach 2017-2018 liczba urządzeń IoT wzrosła o około 3 miliardy, więc pula ataków stała się większa. Jednocześnie notorycznie słaby poziom zabezpieczenia podłączanych do sieci gadżetów zaprasza przestępców do działania.

Wzrost aktywności hakerów jest również widoczny w zestawieniu przedstawiającym miesięczne liczby ataków przeprowadzonych w ciągu ostatnich dwóch lat. Jedynym miesiącem, w którym odnotowano te same wartości w dwóch kolejnych latach, był sierpień. Stało się tak tylko dlatego, że hakerzy urządzili sobie w tym czasie wakacje. Jednak „stratę” tę odrobili z nawiązką w październiku, kiedy to zanotowano co najmniej 8 milionów incydentów.

Po zhakowaniu systemy IoT stają się częścią botnetu, wykorzystywanego w działalności przestępczej. Może on być użyty w atakach typu DDoS (rozproszona odmowa usług), funkcjonować jako kanał przesyłowy dla skradzionych informacji lub po prostu służyć za węzeł pośredniczący w atakach na inne urządzenia. Niektóre ze zhakowanych gadżetów IoT mogą być również używane do przechowywania złośliwego oprogramowania.

Zgodnie z raportem SonicWall, 47% światowych botnetów hostowanych jest w Stanach Zjednoczonych. Na Chiny przypada tu 13%, a na Rosję – zaledwie 7%.

"W wielu przypadkach nie ma wyraźnych oznak, że inteligentny gadżet został zhakowany i służy komu innemu. Niepożądana aktywność może być zazwyczaj powstrzymana przez restart systemu. Jest to też często dobrym sposobem na pozbycie się – rezydującego w systemach IoT – złośliwego oprogramowania, które nie przetrwa takiej operacji. Jednak najpewniejszą metodą dezynfekcji urządzenia jest zwykle przywrócenie domyślnych ustawień fabrycznych" - wyjaśnia Wszebor Kowalski, inżynier techniczny Bitdefender z firmy Marken Systemy Antywirusowe ([https://bitdefender.pl](https://bitdefender.pl/)).