**Już prawie 10 mln ataków dziennie. Polska wśród 25 najbezpieczniejszych miejsc na świecie.**

**Hakerzy na całym świecie próbują atakować komputery i urządzenia osobiste już prawie 10 milionów razy dziennie. Polska jednak opiera się tym próbom i pozostaje w gronie 25 najbardziej bezpiecznych miejsc na świecie (18 w Europie) – wynika z najnowszej analizy firmy Check Point Software Technologies.**

Najnowsza analiza bezpieczeństwa sieciowego oparta o dane z lipca 2018 r., ujawniła znaczny wzrost ataków ukierunkowanych na trzy główne podatności Internetu Rzeczy (IoT). W skali globalnej ataki cybernetyczne najczęściej wymierzone są w tzw. Internet Rzeczy przy wykorzystaniu podatności routerów sieciowych i opierają się na rozprzestrzenianiu złośliwego oprogramowania IoT, takiego jak Mirai, IoTroop/Reaper i VPNFilter. Od maja 2018 ich ilość wzrosła ponad dwukrotnie!

Jak wynika z danych udostępnionych przez firmę Check Point, w lipcu najbezpieczniejszym krajem w Europie, a zarazem na świecie, okazał się Lichtenstein, którego indeks zagrożeń wyniósł zaledwie 12,6 pkt. Wśród krajów europejskich na kolejnych pozycjach podium uplasowały się Szwajcaria (28,9) i Estonia (29,8). Polska w lipcu ulokowała się na 18 pozycji (37,1) w Europie i 25 na całym świecie, dołączając tym samym do grona najbezpieczniejszych krajów. Co ciekawe, w ostatnim czasie ataki na nasze komputery przeprowadzane są głównie z Singapuru (IP komputera) w niedziele i poniedziałki...

W lipcu 2018 r. trzy podatności IoT znalazły się w pierwszej dziesiątce najczęściej wykorzystywanych: Router MVPower DVR router - Zdalne wykonywanie kodów #5; router D\_Link DSL-2750B zdalne wykonywanie poleceń #7; oraz router Dasan GPON z blokadą uwierzytelniania pod numerem 10. Ataki wymierzone w te słabe punkty dotknęły łącznie 45 % organizacji na całym świecie, w porównaniu z 35 % w czerwcu 2018 r. i 21 % w maju. Wszystkie podatności umożliwiają atakującym użycie złośliwego kodu i zdalne sterowanie urządzeniami docelowymi.

- *Znane podatności oferują cyberprzestępcom łatwy, stosunkowo bezproblemowy punkt dostępu do sieci korporacyjnych, umożliwiając im rozprzestrzenianie szerokiego wachlarza ataków* - stwierdziła Maya Horowitz, kierownik grupy analitycznej ds. zagrożeń w punkcie kontrolnym. - *W szczególności luki IoT są często "ścieżką najmniejszego oporu", ponieważ po narażeniu jednego urządzenia na szwank, można łatwo przeniknąć do kolejnych podłączonych urządzeń. W związku z tym ważne jest, aby organizacje stosowały najnowsze poprawki do znanych podatności już w momencie ich udostępniani, co powinno wesprzeć bezpieczeństwo sieci.*

- *W celu ochrony przed zarówno znanymi, jak i nieznanymi podatnościami na ataki cybernetyczne, przedsiębiorstwa muszą stosować wielowarstwową strategię bezpieczeństwa cybernetycznego, która chroni zarówno przed atakami cybernetycznymi z rodzin znanych złośliwych oprogramowań, jak i przed zupełnie nowymi zagrożeniami* - dodała Horowitz.

Najczęściej występującym złośliwym oprogramowaniem na świecie pozostaje Coinhive, który miał wpływ na 19% organizacji na całym świecie. Cryptoloot i Dorkbot zajęły odpowiednio drugie i trzecie miejsce, przy czym każde z nich miało globalny wpływ na poziomie 7 %. W Polsce pierwszy w rankingu popularności był Conficker, który infekował ponad 22% przedsiębiorstw. Na kolejnych pozycjach znalazły się Coinhive (15%) oraz Ramnit (blisko 9%), będący robakiem zarażającym i rozprzestrzeniającym się głównie za pośrednictwem dysków wymiennych i plików przesyłanych do publicznych usług FTP.

Badacze Check Pointa przeprowadzili również analizę najczęściej eksploatowanych podatności cybernetycznych. Liderem okazała się podatność **Microsoft IIS WebDAV** CVE-2017-7269 o łącznym udziale 47%. Drugie miejsce zajęło Apache CVE-2017-5638 o globalnym oddziaływaniu 42%, podium zamknęło z kolei OpenSSL TLS DTLS Heartbeat Information Disclosure, które dotyczy 41% organizacji na całym świecie.