aut. Andrzej Kozłowski 11.07.2019

PONAD 2 MILIONY CYBER INCYDENTÓW W 2018 ROKU. CRYPTOJACKING NA FALI

Internet Society's Online Trust Alliance (OTA) opublikował 11 raport poświęcony incydentom w cyberprzestrzeni, w którym to podsumowano główne trendy, jeśli chodzi o zagrożenia w Internecie w 2018 roku oraz przedstawiono szereg rekomendacji dla organizacji, aby przeciwdziałać cyberatakom i ograniczać ich skutek. Dokument ten przedstawia również zmianę krajobrazu zagrożeń.

OTA oszacowała, że w 2018 roku doszło do około 2 milionów cyberincydentów. Autorzy raportu uważają, iż rzeczywiście było ich o wiele więcej, ale duża część z nich nie została odnotowana. Według nich koszty działalności cyberprzestępców wynoszą 45 miliardów dolarów rocznie. Głównymi rodzajami ataków jest cryptojacking, ransomware, ataki na łańcuch dostaw, naruszenia danych oraz ataki BEC (Business Email Compromise). OTA stwierdza, że istnieje wiele organizacji śledzących wycieki danych. Przykładowo Risk Based Security stwierdza, że od 2017 roku było ponad 6 tys. danych tego typu incydentów, w wyniku których wyciekło ponad 5 miliardów rekordów. Oczywiście te obliczenia różnią się w zależności od przyjętej metodologii.

Autorzy raportu zauważają, że liczba ataków ransomware maleje, ale nie wiąże się to ze spadkiem strat finansowych poniesionych ze względu na ten rodzaj działalności hakerów. Dobrze znane ataki typu DDOS również nie odeszły w zapomnienie. W 2018 roku ich ofiarą padły banki, serwisy edukacyjne a także popularne serwisy takie jak ProtonMail czy GitHub. Analizując poszczególne rodzaje zagrożeń, autorzy przytoczyli wyniki badań innych organizacji i firm.

Odnosząc się do zagrożenia dla firm, wskazano BEC jako rosnące zagrożenie, gdzie pracownicy coraz częściej są oszukiwaniprzez atakujących, w następnie czego wysyłają im pieniądze. Według raport FBI „Internet Crime Report" z 2018 roku, ponad 20 tys. incydentów tego typu zanotowano w samych Stanach Zjednoczonych, co doprowadziło do strat rzędu 1,4 miliardów. W 2016 roku liczba takich incydentów była niższa i wynosiła 16 tys., które przyniosły straty w wysokości 677 milionów dolarów.

Najpopularniejsza w tym roku forma ataków, czyli cryptojacking, zdecydowanie wzrosła w porównaniu do 2017 roku. Według Trend Micro było ich trzykrotnie więcej. Symantec Internet Security Threat Report alarmuje również że o prawie 80% wzrosła liczba ataków na łańcuch dostaw w porównaniu do roku 2017.

Inne kategorie ataków związane są ze zmieniającą się infrastrukturą Internetu. Coraz więcej firm przenosi swoje operacje do chmury, co powoduje, że te stają się coraz częściej celem ataku. Według wyliczeń Digital Shadows na świecie było półtora miliarda plików, które były narażone na kradzież ze względu na złą konfigurację serwisów chmurowych.

Urządzenia Internetu Rzeczy coraz częściej stają się narzędziem przeprowadzania różnych typów cyberataków, poczynając od DDoS do cryptojackingu. Kapersky Lab twierdzi, że w ostatniej połowie 2018 roku, zaobserwowano trzykrotny wzrost w liczbie złośliwego oprogramowania, które używane

jest do infekowania urządzeń IoT.

Raport również przedstawia szereg rekomendacji, które powinny wdrożyć organizacje tak, aby chronić się przed incydentami oraz ograniczać ich potencjalne, negatywne skutki. Organizacje mogą wykorzystać schemat OTA IoT Trust do poprawy bezpieczeństwa ekosystemu IoT.

Krajobraz zagrożeń stale się rozwija, pojawiają się nowe rodzaje ataków, a liczba starych stale rośnie. Organizacje muszą być czujne i świadome zagrożeń. Przede wszystkim jednak członkowie zarządu muszą pogodzić się z myślą, że prędzej czy później dojdzie do sytuacji, w której będą musiały one sobie radzić z incydentami w cyberprzestrzeni.

Źródło: Internet Society’s Online Trust Alliance