

Ponad połowa polskich komputerów jest zainfekowana wirusami i trojanami. To daje Polsce 12. miejsce na świecie i stwarza poważne niebezpieczeństwo, bo zaatakowane komputery stają się tzw. zombie, czyli sprzętem opanowanym przez cyberprzestępców, który służy do atakowania kolejnych komputerów. O skali zagrożenia ze strony złośliwego oprogramowania świadczą m.in. ogromne straty sięgające 5,5 mld dol, które spowodował wirus Iloveyou.

Cyberprzestępcy udoskonalają swoją działalność, co oznacza, że straty spowodowane ich działalnością będą stale rosły.

Do krajów najbardziej narażonych na infekcję komputerowymi wirusami należą m.in. Tajlandia, Chiny i Tajwan, gdzie od 60 do 70 proc. komputerów jest zarażonych przez cyberprzestępców. W Polsce niemal co drugi użytkowany komputer jest zainfekowany złośliwym oprogramowaniem, z tego powodu nasz kraj znajduje się w światowej czołówce państw, gdzie to zjawisko nasila się w największym stopniu.

Niestety pokaźna ilość użytkowników komputerów w naszym kraju wciąż oszczędza na programach antywirusowych. Są to tylko pozorne oszczędności, które ułatwiają dokonanie włamań cyberprzestępcom. Równie istotne znaczenie ma ciągle bardzo duża popularność nielegalnego oprogramowania w naszym kraju. Między innymi z tego powodu w Polsce mamy do czynienia z tak dużą ilością komputerów zainfekowanych złośliwym oprogramowaniem – mówi Krzysztof Seweryn, prezes zarządu InwazjaPC, spółki będącej jednym z liderów w sprzedaży notebooków w Polsce. – Ofiary wirusów często nie wiedzą, że ich sprzęt został zainfekowany. Szkodliwe aplikacje tworzone są tak, aby ich działanie było niezauważalne dla użytkowników zainfekowanych komputerów. Coraz częściej wirusy atakują też smartfony.

Zbyt niski poziom zabezpieczeń antywirusowych nie jest jedynie domeną prywatnych użytkowników sprzętu komputerowego w Polsce. Również firmy, szczególnie mniejsze, bagatelizują ten problem. Taka sytuacja ułatwia działania przestępcom, którzy są coraz lepiej zorganizowani. Coraz częściej wykorzystują także portale społecznościowe m.in. do pozycjonowania fałszywych stron www. Dynamiczny rozwój mediów społecznościowych stanowi dla cyberprzestępców bardzo sprzyjające zjawisko, które ułatwia intensyfikację ich procederu.

Wirusy bezpośrednio nie uszkadzają sprzętu komputerowego, ale skutki ich działań mogą być bardzo poważne. Złośliwe oprogramowanie może doprowadzić do całkowitego zniszczenia wszystkich informacji zapisanych w komputerze. Wirusy mogą umożliwić kradzież licznych danych np. haseł do kont bankowych, mogą także nabić rachunek telefoniczny właściciela zainfekowanego komputera, przekierowując połączenie modemowe na płatne numery. Coraz więcej jest też wirusów dedykowanych urządzeniom mobilnym: smartfonom i tabletom. W tym przypadku złośliwe oprogramowanie powoduje m.in. wysyłanie dużej ilości sms-ów bez wiedzy właściciela urządzenia.

Pierwszy wirus-Brain został wykryty w styczniu 1986 roku, w porównaniu z jego następcami powodował on jedynie niegroźne komplikacje w sektorach startowych komputerów. Twórcy złośliwego oprogramowania dość szybko zintensyfikowali swoją działalność, tworząc e-mailowe robaki. Najbardziej znanym był wykryty w 2000 roku Iloveyou, który spowodował straty sięgające 5,5 mld dolarów. Zagrożenie na globalną skalę spowodowały sieciowe robaki, które wykorzystują luki w zabezpieczeniach systemów i replikują się same bez konieczności współpracy użytkownika. Pierwszy taki wirus – Code Red został wykryty w 2001 roku, spowodował atak m.in. na sieć informatyczną Białego Domu.

BADOG