**Polska nadal poza 20 najbezpieczniejszych krajów Europy w rankingu bezpieczeństwa sieciowego. Cryptominery podkopujące moc obliczeniową komputerów w firmach nadal stanowią zagrożenie.**

**Polska znalazła się wśród bardzo niebezpiecznych miejsc pod względem ataków hakerów. Nasz kraj jest dopiero na 22 pozycji w Europie – informują analitycy firmy Check Point Software Technologies. Hakerzy coraz częściej wykorzystują tzw. cryptominers, wykorzystujące nawet 65% mocy obliczeniowej procesorów w naszych komputerach.**

*- Pozycja Polski jest nadal odległa od ideału. Nasz kraj znajduje się poza pierwszą 20 najbardziej bezpiecznych (22) w rankingu europejskim, uzyskując przy tym indeks zagrożeń równy 42,7 pkt. Oznacza to, że aktywność hakerów skierowana przeciwko polskim firmom i użytkownikom indywidualnym utrzymuje się na wysokim poziomie. Zagrożeniem są Cryptominery,**podkopujące moc obliczeniową komputerów w firmach.* – podkreśla Wojciech Głażewski, dyrektor zarządzający firmy Check Point w Polsce.

Według danych Check Point 42% organizacji na całym świecie zostało zainfekowanych tym, złośliwym oprogramowaniem. Najbezpieczniejszym krajem w lutym ponownie okazał się Lichtenstein (10,4 punktu w indeksie zagrożeń). Na kolejnych pozycjach znalazły się Cypr (28,9) oraz Norwegia (29,3). Najbardziej zagrożonymi państwami są obecnie Estonia (76,8) oraz Macedonia (76).

W najnowszym raporcie przedstawiono m.in. najpopularniejsze na świecie złośliwe oprogramowanie wykorzystywane przez hakerów. Badaczom Check Pointa udało się wykryć aż trzy różne warianty cryptominers. Podczas gdy Coinhive utrzymał pierwsze miejsce, infekując nawet jedną piątą organizacji na całym świecie, Cryptoloot awansował na drugie miejsce po podwojeniu globalnej infekcji z 7% w styczniu do 16% w lutym. Zestaw Rig Exploit Kit zajął trzecie miejsce, a jego zakres infekcji osiągnął 15% wszystkich organizacji.

W Polsce sytuacja nieznacznie się różni: najpopularniejszym typem malware jest kampania malvertisingowa Roughted, która awansowała z trzeciej na pierwszą pozycję. Na drugim miejscu ulokował się światowy lider – Coinhive; z kolei podium zamyka Necrus, będący jednym z największych botnetów na świecie.

*- W ciągu ostatnich czterech miesięcy w dalszym ciągu rośnie rozpowszechnienie malware’u wykorzystywanego do kopania kryptowalut. To uporczywe zagrożenie nie tylko spowalnia pracę komputerów i serwerów, ale po penetracji sieci przez tych agentów, mogą one być również wykorzystane do wykonywania innych złośliwych czynów. Dlatego niezwykle ważne jest aby przedsiębiorstwa stosowały wielowarstwową strategię bezpieczeństwa cybernetycznego, która chroni zarówno przed istniejącymi rodzinami złośliwego oprogramowania, jak i nowymi zagrożeniami.* – twierdzi Maya Horowitz, kierownik Threat Intelligence Group w Check Point Software Technologies.

Od ostatnich czterech miesięcy, tzw. „cryptomining malware” jest stale rosnącym zagrożeniem dla organizacji, ponieważ wciąż jest bardzo lukratywnym narzędziem dla przestępców. Oprócz spowolnienia pracy komputerów i serwerów, ma możliwość wykonywania innych szkodliwych działań po wejściu do systemu. Kluczowe znaczenie ma to, aby organizacje dysponowały rozwiązaniami zabezpieczającymi przed nowymi, zakrojonymi na szeroką skalę i szybko przemieszczającymi się atakami cybernetycznymi piątej generacji.