**Cyberprzestępcy atakują częściej Rosję, Czechy i Niemcy. Polska wśród 16 najbezpieczniejszych krajów w Europie.**

**Codziennie hakerzy dopuszczają się ponad 12 milionów ataków na użytkowników sieci Internet na świecie. To wzrost o 20 proc. w stosunku do czerwca 2018 roku. Najbezpieczniejszym miejscem został uznany Lichtenstein - zarówno w Europie jak i na świecie - indeks zagrożeń wyniósł w tym kraju zaledwie 11,4 punktu – oznaczało to w skali globalnej awans aż o 129 miejsc, względem wrześniowego rankingu! Na drugim miejscu – pod względem bezpieczeństwa sieciowego - uplasowała się Norwegia (25,4), na trzecim Finlandia (28,8) - to wnioski płynące z najnowszych analiz firmy Check Point Software Technologies.**

**Polska znalazła się na 16 miejscu w Europie i 25 na świecie (awans o 3 pozycje). Nasz indeks wyniósł 33,4 punktu, co pozwoliło nam wyprzedzić m.in. Rosję (33,4), Czechy (33,6) czy Niemcy (33,9).** Polscy użytkownicy komputerów najczęściej atakowani są w niedziele przez hakerów z niemieckim adresem IP.

**Cyberbezpieczeństwo: Trojany zdalnego dostępu w natarciu!**

Analitycy Check Point są zgodni – do najczęściej wykorzystywanego złośliwego oprogramowania należą kryptominery, natomiast na znaczeniu coraz bardziej zyskują RAT-y, czyli trojany zdalnego dostępu.

Po raz pierwszy w historii tzw. globalnego indeksu zagrożeń firmy Check Point, trojany zdalnego dostępu (RAT) znalazły się w pierwszej dziesiątce najpowszechniejszych zagrożeń cyberprzestrzeni. Jeden z nich – FlawedAmmyy – pozwala napastnikowi zdalnie kontrolować maszynę ofiary, uzyskać pełny dostęp do kamery i mikrofonu maszyny, dokonywać zrzutów ekranu, jednocześnie kradnąc dane uwierzytelniające i wrażliwe pliki.

W ciągu ostatnich kilku miesięcy, badacze Check Point zaobserwowali szereg kampanii rozpowszechniających FlawedAmmy, natomiast w październiku br. odkryto największą z nich – rozmiarami przekraczającą dotychczas obserwowane kampanie wykorzystujące ten typ trojanów. Była ona na tyle duża, że pozwoliła FlawedAmm RAT na dołączenie do czołowej dziesiątki najliczniejszych zagrożeń czyhających w Internecie.

Najpopularniejszym typem złośliwego oprogramowania wciąż są kryptominery, czyli narzędzia do nielegalnego generowania kryptowalut, wykorzystujące moce obliczeniowe komputerów ofiar. Najbardziej rozpowszechnionym z nich jest Coinhive, który wykrywany był w 18% korporacji na całym świecie. Drugi pod względem powszechności to Cryptoot, z zasięgiem ponad 8% - oba kryptominery zajmują dwie pierwsze pozycje w rankingu najpopularniejszych typów malware. Podium zamyka Dorkbot, będący robakiem opartym o protokół IRC.

**TOP 3 malware na świecie:**

1. **Coinhive** – Crypominer przeznaczony do wydobywania kryptowaluty Monero bez zgody użytkownika odwiedzającego stronę internetową. Coinhive pojawił się dopiero we wrześniu 2017 r., ale już w tym czasie infekował 12% organizacji na całym świecie.

1. **Cryptoloot** – Cryptominer wykorzystujący moc procesora lub procesora graficznego ofiary oraz istniejące zasoby do wytworzenia nowej waluty. Dodaje transakcje do tzw. Blockchainu, wprowadzając nową walutę.

1. **Dorkbot-** Oparty na IRC robak umożliwiający zdalne wykonywanie kodu przez operatora oraz pobieranie dodatkowego złośliwego oprogramowania do zainfekowanego systemu. Jest to bankowy trojan, którego głównym zadaniem jest kradzież poufnych informacji i przeprowadzanie ataków typu denial-of-service.

W przypadku urządzeń mobilnych, znów czołowe pozycje zajmuje jedynie malware skierowany przeciwko Androidowi. Triada, modułowy backdoor, wspiął się na pierwsze miejsce na liście najczęstszych mobilnych złośliwych programów. Zastępuje on trojana bankowego i złodzieja danych – Lokibot, który spadł na drugie miejsce. Hiddad powrócił z kolei na listę jako trzecie najbardziej rozpowszechnione mobilne złośliwe oprogramowanie w tym miesiącu.

Badacze z Check Pointa przeanalizowali również najbardziej wykorzystywane luki w cyberprzestrzeni. Po raz kolejny CVE-2017-7269 pozostaje na pierwszym miejscu listy najczęściej wykorzystywanych luk w zabezpieczeniach, z globalnym wpływem na 48% organizacji. Na drugim miejscu znalazło się OpenSSL TLS DTLS Heartbeat Information Disclosure o globalnym wpływie 46%, a następnie Web servers PHPMyAdmin Misconfiguration Code Injection zidentyfikowany w 42% organizacji.