**Polska poza 20. europejskiego rankingu bezpieczeństwa cybernetycznego!**

**Hakerzy coraz częściej staje się celem ataków hakerów. W konsekwencji nasz kraj spada europejskich rankingu bezpieczeństwa sieciowego na 22 miejsce - wskazują dane firmy Check Point. Najlepiej pod tym względem wypada Irlandia, Szewcja oraz Serbia; najgorzej – Macedonia. Eksperci zaznaczają, że w lutym nastąpił duży wzrost wykorzystania exploitów w celach rozprzestrzeniania botnetu Mirai, który jest znany z infekowania urządzeń IoT i przeprowadzania masowych ataków DDoS.**

Firma Check Point przedstawiła najnowsze dane (luty 2020) dotyczące horyzontu zagrożeń cybernetycznych. Irlandia (indeks zagrożeń (26,4), Szwecja (31,6) oraz Serbia (32,5) to czołowa trójka najbezpieczniejszych sieci w Europie. Tym razem Polska zajęła dopiero 22 pozycję (40,7) i wyprzedzona została m.in. przez Królestwo Niederlandów, Słowenię czy Maltę. Więcej skutecznych działań hakerskich odnotowano m.in. w Portugalii (40,9) oraz Francji (41,3). Z kolei za najniebezpieczniejszą w Europie ponownie została uznana sieć macedońska, z indeksem zagrożeń na poziomie 68,4.

Zespół badawczy Check Pointa ostrzega również, że Emotet, drugie najpopularniejsze szkodliwe oprogramowanie w tym miesiącu i najbardziej rozpowszechniony działający obecnie botnet, rozprzestrzenia się za pomocą dwóch nowych wektorów. Pierwszym z nich była kampania typu SMS phishing (smishing), skierowana przeciwko amerykańskim użytkownikom. SMS podszywa się pod wiadomości z popularnych banków, zachęcając ofiary do kliknięcia złośliwego linku, który pobiera Emotet na urządzenie. Drugim wektorem jest Emotet wykrywający i wykorzystujący pobliskie sieci Wi-Fi w celu rozprzestrzeniania się za pomocą ataków siłowych (brute force) przy użyciu szeregu często używanych haseł Wi-Fi. Emotet jest wykorzystywany głównie jako dystrybutor oprogramowania ransomware oraz innych złośliwych kampanii.

Emotet wpłynął w lutym na ponad 6% organizacji na całym świecie, w porównaniu z 13% w styczniu, kiedy rozprzestrzeniał się głównie poprzez kampanię spamową o tematyce koronawirusa. Pokazuje to, jak szybko cyberprzestępcy zmieniają tematy ataków, próbując zmaksymalizować liczbę infekcji.

*- Wydaje się, że przestępcy dążą do zbudowania jak największej sieci zainfekowanych urządzeń, które mogą następnie wykorzystywać i zarabiać na wiele różnych sposobów, od dostarczania oprogramowania ransomware do przeprowadzania ataków DDoS* - powiedziała Maya Horowitz, dyrektor ds. Analiz i badań zagrożeń w Check Point.

**Czołowe rodziny malware’u w lutym ‘20**

W tym miesiącu na pierwszym miejscu na świecie ulokował się XMRig z wpływem na 7% organizacji. Za nim umiejscowiły się Emotet I Jsecoin z infekcjami na poziomie 6% i 5%.

1.  **↑ XMRig** - cryptominer, który dzięki pracy bezpośrednio na urządzeniu końcowym, a nie na samej przeglądarce internetowej jest w stanie wykopywać kryptowalutę Monero bez potrzeby sesji aktywnej przeglądarki internetowej na komputerze ofiary. Wykryty po raz pierwszy w maju 2017 roku.

2.  **↓ Emotet** – zaawansowany, samoreplikujący się i modułowy trojan. Znany wcześniej jako trojan bankowy, ostatnio wykorzystywany jako dystrybutor innego złośliwego oprogramowania lub złośliwych kampanii. Wykorzystuje wiele technik unikania wykrycia. Ponadto można go rozprzestrzeniać za pośrednictwem wiadomości e-mail zawierających spam typu phishing, zawierających złośliwe załączniki lub łącza.

3. **↑Jsecoin** - cryptominer JavaScript, który może być osadzony na stronach internetowych. JSEcoin może uruchomić koparkę bezpośrednio w przeglądarce.

W Polsce w zeszłym miesiącu wiodącym szkodnikiem był Formbook, czyli trojan typu infostealer na Windowsa, przechwytujący dane z klawiatury oraz robiący zrzuty ekranu. Ten rodzaj malware’u zainfekował około 6,5% sieci. Na drugim miejscu uplasował się Emotet (6,5%) oraz trojan bankowy Trickbot (blisko 6,2%).

**Czołowe rodziny malware’u mobilnego w lutym ‘20**

W lutym na pozycji światowego lidera zarażeń urządzeń mobilnych pozostał xHelper, wyprzedzając Hiddad i Guerilla.

1. **↔**xHelper **-** Złośliwa aplikacja na Androida, która pojawiała się w marcu 2019 r., Używana do pobierania innych złośliwych aplikacji i wyświetlania reklam. Aplikacja może ukrywać się przed użytkownikami i mobilnymi programami antywirusowymi i instaluje się ponownie, jeśli użytkownik ją odinstaluje.

2. **↑**Hiddad- Złośliwe oprogramowanie na Androida, które przepakowuje legalne aplikacje, a następnie udostępnia je do sklepu osób trzecich. Jest w stanie uzyskać dostęp do kluczowych szczegółów bezpieczeństwa wbudowanych w system operacyjny, co pozwala atakującemu na uzyskanie poufnych danych użytkownika.

3. **↓**Guerrilla- Trojan na Androida, który znalazł się w wielu legalnych aplikacjach. Może pobierać dodatkowe złośliwe ładunki. Generuje przychody z fałszywych reklam dla twórców aplikacji.