**Check Point: Polska najbardziej zagrożonym krajem Unii Europejskiej!**

**Według najnowszego zestawienia rankingu cyberzagrożeń firmy Check Point Software Technlologies, Polska była najbardziej podatnym na ataki hakerskie krajem Unii Europejskiej. Z udostępnionych danych wynika, że w listopadzie ulokowaliśmy się na 34. miejscu wśród najczęściej atakowanych państw świata, z kolei najczęstszym narzędziem wykorzystywanym przez hakerów jest bezzmiennie Conticker!**

W oparciu o dane z [ThreatCloud World Cyber Threat Map](https://www.threat-cloud.com/ThreatPortal/#/map), mapy cyberzagrożeń ukazującej w czasie rzeczywistym miejsca i sposoby przeprowadzania cyberataków, firma Check Point zidentyfikowała w listopadzie ponad 1200 różnych rodzin złośliwego oprogramowania. Trzema najczęściej atakującymi rodzinami malware, odpowiadającymi za niemal 40% wszystkich rozpoznanych ataków, były odpowiednio:

**↔ Conficker** – odpowiada za 20% wszystkich rozpoznanych ataków, urządzenia zainfekowane przez takie oprogramowanie są kontrolowane przez botnet. Wyłącza usługi zabezpieczeń, co naraża komputery na inne infekcje.

↑ **Cutwail** – botnet używany głównie do rozsyłania spamu oraz ataków DDos.

**↑ Necurs** - używany jako backdoor do pobierania kolejnych złośliwych programów na zainfekowane urządzenie oraz do wyłączania usług zabezpieczeń, aby uniemożliwić jego wykrycie.

Badania ujawniły również globalny 17% wzrost w użyciu złośliwego oprogramowania na urządzeniach mobilnych w listopadzie. Za ataki na urządzenia mobilne najczęściej odpowiadały trzy rodziny malwarte - Xinyin, Ztorg i AndroRAT. Liczba ataków przy pomocy Xinyin i AndroRAT zwiększyła się około dwukrotnie w porównaniu z poprzednim miesiącem, zaś w przypadku AndroRAT wzrost był aż 10-cio krotny! Wszystkie trzy rodzaje wycelowane są w urządzenia z systemem Android.

1. **↑ Xinyin** – obserwowany jako trojan clicker wykonujący fałszywe kliknięcia na chińskich stronach reklamowych.

2. **↓ Ztorg** – trojan wykorzystujący uprawnienia użytkownika root w celu pobierania i instalowania aplikacji na telefonie komórkowym bez wiedzy użytkownika.

3. **↑ AndroRAT** – złośliwe oprogramowanie, które może zostać pobrane wraz z legalną aplikacją mobilną i zainstalowane bez wiedzy użytkownika, dając hakerowi pełną zdalną kontrolę nad urządzeniem z systemem Android.

**Polska wśród najbardziej zagrożonych**

Według najnowszych danych, Polska zajęła niechlubną, pierwszą pozycję wśród państw Unii Europejskiej, wyprzedzając m.in. Grecję czy Włochy. W klasyfikacji uwzględniającej wszystkie kraje świata uplasowaliśmy się na 34 miejscu – trzy oczka niżej niż w zestawieniu sprzed miesiąca, jednak współczynnik zagrożenia naszych komputerów wzrósł z 9,2 do 17,2 pkt. Najbardziej zagrożonymi maszynami, okazały się te podłączone do sieci w Arabii Saudyjskiej i Namibii.

*Każdego dnia organizacje walczą o ochronę swoich sieci przed cyberprzestępcami, dlatego niezmiernie ważne jest, aby miały świadomość tego, z czym muszą się mierzyć. Dane z listopada wskazują, że atakujący koncentrują się na złośliwym oprogramowaniu, które może wyłączyć usługi zabezpieczeń i ukradkiem zainfekować urządzenia, ułatwiając ich wykorzystywanie* – **stwierdził Nathan Shuchami**, szef działu Ochrony przed zagrożeniami w firmie Check Point.

*Wzrost obecności złośliwego oprogramowania wskazuje również na zwiększoną potrzebę ochrony przez organizacje urządzeń mobilnych używanych przez ich pracowników, które zawierają cenne dane firmowe. Atakujący zrozumieli, że te urządzenia są łatwiejszym celem niż sieci firmowe, dlatego tak ważne jest, aby organizacje zadbały o ich ochronę przed wykorzystywaniem i wyciekiem danych* – dodał Shuchami.

Jak wynika z opublikowanego przez firmę Check Point „Security Report 2015”, w zeszłym roku co godzinę dochodziło średnio do 106 różnego rodzaju ataków wymierzonych w organizacje na całym świecie. To 48 razy częściej niż w roku poprzedzającym 2014! Według ekspertów, cyberprzestępcy do wykradania danych osobistych coraz częściej korzystają z luk aplikacji antywirusowych oraz programów typu „bot”, które w 2014 roku zaatakowały aż 83% firm.

Wszystkie przedstawione przez firmę Check Point dane pochodzą z analiz ThreatCloud, największej sieci współpracy ukierunkowanej na walkę z cyberprzestępczością. ThreatCloud zawiera ponad 250 mln adresów analizowanych pod kątem obecności botów, 11 mln sygnatur złośliwego oprogramowania i ponad 5,5 mln zainfekowanych stron internetowych, wykrywa też miliony rodzajów złośliwego oprogramowania każdego dnia.