**Polska na celowniku hakerów: Emotet głównym zagrożeniem dla polskich organizacji.**

**We wrześniu nastąpił drastyczny wzrost zagrożeń ze strony cyberprzestępców lokując Polskę dopiero na niskim - 20 miejscu europejskiego rankingu bezpieczeństwa. Głównym zagrożeniem zarówno dla sieci firmowych, jak i użytkowników indywidualnych były kampanie spamowe ze złośliwymi załącznikami, przeprowadzane za pomocą botnetu Emotet - donoszą specjaliści ds. cyberbezpieczeństwa firmy Check Point.**

Dania, Finlandia i Luksemburg to obecnie trzy najbezpieczniejsze sieci w Europie. Na przeciwległym krańcu rankingu znajdują się z kolei Macedonia oraz Gruzja, które są najniebezpieczniejszymi miejscami dla internautów nie tylko w skali Europy, ale również wśród najbardziej niebezpiecznych na świecie!

Wg ekspertów Check Point Research, wrzesień był dla polskiej sieci miesiącem zintensyfikowanych ataków, głównie za pośrednictwem kampanii spamowych. W rezultacie nasz kraj zajął dopiero 20 miejsce w zestawieniu, uzyskując indeks zagrożeń na poziomie 40,6 punktu. W klasyfikacji europejskiej wyprzedziły nas m.in. Słowenia (35,4), Słowacja (39,1) czy Francja (40,2), natomiast w skali świata również Bangladesz i Kambodża! Za naszymi plecami ulokowały się min. Serbia (41,8), Cypr (41,9) czy Węgry (42,7).

**Emotet powrócił**

Botnet Emotet na dobre wznowił działalność po trzymiesięcznej przerwie, która nastąpiła w czerwcu br. i natychmiast wskoczył na pierwsze miejsce w Polsce i piątą pozycję światowej listy najbardziej rozpowszechnionych typów złośliwego oprogramowania.

Specjaliści ds. bezpieczeństwa, po analizach aktywności cyberprzestępców, już w sierpniu zapowiadali ofensywę hakerską z wykorzystaniem tego narzędzia. Nowe kampanie spamowe dokonywane za pomocą Emotetu rozsyłały wiadomości e-mail zawierające link do pobrania złośliwego pliku Word, a inne zawierały sam szkodliwy dokument. Po otwarciu pliku ofiary przekonywane były by włączyć makra dokumentu, które następnie instalowały złośliwe oprogramowanie.

**Czołowy malware i podatności**

W tym miesiącu Jsecoin jest liderem na liście najpopularniejszych szkodliwych programów, wpływając na 8% organizacji na całym świecie. XMRig jest drugim najpopularniejszym złośliwym oprogramowaniem, a za nim znajduje się AgentTesla, oba o globalnym wpływie 7%.

1. **Jsecoin** – cryptominer JavaScript, który może być osadzony na stronach internetowych. JSEcoin może uruchomić koparkę bezpośrednio w przeglądarce.

2. **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.

3. **Agentesla** –zaawansowany trojan zdalnego dostępu (RAT), funkcjonujący jako keylogger I złodziej haseł. Jest w stanie monitorować i zbierać dane z klawiatury ofiary, schowka systemowego, robić zrzuty ekranu i wyciągania poświadczeń należących do różnych programów zainstalowanych na urządzeniu

W Polsce najczęściej wykorzystywanym malware (11,38%) był wspomniany Emotet, co potwierdzają działy IT polskich firm, donoszące o lawinowym wzroście ilości otrzymywanego spamu. Na drugim miejscu znalazł się cryptominer Jsecoin (10,69%), natomiast podium zamknął Agenttesla (9,31%)

Wśród podatności najczęściej wykorzystywana była MVPower DVR Remote Code Execution, wykorzystywana w przypadku 37% zaatakowanych organizacji. Drugą była luka w zabezpieczeniach systemów Linux - The Linux System Files Information Disclosure – razem z Web Server Exposed Git Repository Information Disclosure, które dotyczyły po 35% przedsiębiorstw. Kolejne miejsce zajęło popularne SQL Injection.