**Polska sieć pożywką dla hakerów!**

**W kwietniu nastąpił znaczny wzrost ataków na polskie komputery. Najnowsze badanie firmy Check Point wskazują, że Polska znajduje się na szarym końcu (27 miejsce) europejskiego rankingu bezpieczeństwa sieciowego. Kwiecień był najgorszym okresem dla polskich internautów od wielu miesięcy m.in. za sprawą kolejnych niebezpiecznych kampanii spamowych wykorzystujących temat koronawirusa.**

Irlandia i Wielka Brytania to obecnie dwa najbezpieczniejsze kraje w Europie pod względem bezpieczeństwa sieciowego. Najbardziej niebezpieczne to Litwa i Łotwa. Polska, znalazła się w dopiero w trzeciej dziesiątce rankingu (miejsce 27) – wynika z danych przedstawionych przez Check Point Research. **Z indeksem zagrożeń na poziomie 46,5 pkt., nasz kraj znalazł się w TOP 50 (47 miejsce) państw o najwyższym poziomie zagrożeń na świecie!**

Analiza bieżących zagrożeń cybernetycznych wykazała, że hakerzy wciąż chętnie wykorzystują do ataków kampanie spamowe związane z koronawirusem (COVID-19). W kwietniu za ich pomocą starali się dystrybuować nowy wariant trojana zdalnego dostępu Agent Tesla, który uplasował się na trzecim miejscu listy najpowszechniejszego malware, wpływając na 3 % organizacji na całym świecie.

Nowy wariant Agenta Tesla został zmodyfikowany w celu kradzieży haseł Wi-Fi oraz innych informacji - takich jak poświadczenia e-mail programu Outlook. Jedna z tego typu kampanii podszywała się pod Światową Organizację Zdrowia (WHO), a w temacie wiadomości pojawił się tytuł:

**„*PILNE LISTY INFORMACYJNE: PIERWSZY TEST SZCZEPIONKI COVID-19 DLA LUDZI - WYNIKI/AKTUALIZACJA WYNIKÓW”.***

Sposób dystrybucji pokazuje w jaki sposób hakerzy wykorzystają globalne wydarzenia i obawy opinii publicznej, aby zwiększyć sukces ataku.

Choć kampanie spamowe wykorzystujące Agenta Tesla rosną w siłę, globalnym numerem jeden był trojan bankowy Dridex (wykryty w 4% firm na świecie). To jednocześnie najczęściej wykorzystywane oprogramowanie do ataków na polskie firmy. W przypadku polskiej sieci Dridex spadł w kwietniu z pierwszego na czwarte miejsce *„najpopularniejszych szkodników”* z udziałem na poziomie 2,4%. Tym razem najpowszechniejszym zagrożeniem w polskich organizacjach okazał się trojan Emotet.

- *Kampanie malspamowe (*od malware + spam – przyp. red.*) Agent Tesla, które wykryliśmy w kwietniu, podkreślają, jak elastyczni mogą być cyberprzestępcy, jeśli chodzi o wykorzystywanie wydarzeń informacyjnych i nakłanianie niczego niepodejrzewających ofiar do kliknięcia zainfekowanego łącza* - powiedziała Maya Horowitz, dyrektor ds. Analizy i badań zagrożeń w Check Point Software Technologies

- *Wykorzystując Agenta Tesla, jak i Dridex, przestępcy koncentrują się na kradzieży danych osobowych i biznesowych użytkowników, by móc wykorzystać je w celach zarobkowych. Stąd ważne jest, aby organizacje przyjęły proaktywne i dynamiczne podejście do edukacji użytkowników, informując swoich pracowników o najnowszych narzędziach i technikach, zwłaszcza że większość pracowników pracuje obecnie z domów.*

Zespół badawczy ostrzega również przed powszechnymi podatnościami w systemach komputerowych. „Zdalne wykonanie kodu MVPower DVR” pozostaje najczęstszą wykorzystywaną luką, a jej zakres zwiększył się w ostatnich tygodniach, obejmując 46% organizacji na całym świecie. Zaraz za nią uplasował się “OpenSSL TLS DTLS Heartbeat Information Disclosure” o globalnym wpływie 41%, natomiast trzecią najpowszechniejszą podatnością jest “Command Injection Over HTTP Payload” wykorzystywaną w przypadku 40% organizacji na całym świecie.

Pełna lista zagrożeń dostępna jest na [blogu firmy Check Point](https://blog.checkpoint.com/2020/05/11/april-2020s-most-wanted-malware-agent-tesla-remote-access-trojan-spreading-widely-in-covid-19-related-spam-campaigns/).