Artykuł **„Patryk Vega, polski komunikator i Mosad. Co tu się w ogóle wydarzyło?”**, opublikowany w czasopiśmie **„Antyweb.pl”** w dniu 11 lutego 2021 r., zawiera **nieprawdziwe informacje** na temat aplikacji Usecrypt Messenger. W sposób sprzeczny z faktami, sugeruje, że:

1	NIEPRAWDZIWA INFORMACJA W ARTYKULE: Patryk Vega jest mistrzem Polski robienia szumu wokół siebie i swoich filmów. Tym razem postanowił jednak wykorzystać swoją „technikę” do **zareklamowania polskiego** komunikatora UseCrypt Messenger, który ma zapewniać tak wysoki poziom bezpieczeństwa, że nawet Mosad nie zdołał go złamać.	**Nieprawdą jest, że jest to reklama.** Pan Patryk Vega nie jest stroną żadnej umowy reklamowej z Usecrypt. **Jest to kampania społeczna.** Usecrypt Messenger nie jest polskim komunikatorem. W kwietniu 2019 technologia została kupiona przez amerykańsko-izraelski fundusz: https://ceo.com.pl/usecrypt-wykupiony-przez-lazar-vision-fund-27271
2	NIEPRAWDZIWA INFORMACJA W ARTYKULE: UseCrypt Messenger to polski komunikator **bazujący na protokołach Signala z dodatkiem własnych rozwiązań**, o którym jakiś czas temu zrobiło się głośno w wyniku ich kontrowersyjnej kampanii marketingowej.	**Usecrypt Messenger posiada własną aplikacje do rozmów głosowych oraz sprawdzania bezpieczeństwa telefonu,** za którą pobierana jest opłata. Fragment kodu Signala został wykorzystany, jedynie w warstwie tekstowej aplikacji. Został znacznie poprawiony i rozbudowany. (Szczegóły przekazane do wglądu Redakcji) Usecrypt złożył 4 wnioski patentowe i uzyskał ochronę „dniem pierwszeństwa” potwierdzając unikalność własnych rozwiązań, dotyczących zabezpieczenia danych w aplikacji na aparacie użytkownika, czego kompletnie nie posiada Signal, ani żaden inny komunikator (Informacje o etapie postępowania patentowego przekazane Redakcji): 1. Kontrola Bezpieczeństwa 2. Enter code wraz szyfrowaniem bazy aplikacji na telefonie 3. Panic code Szczegóły licencji Usecrypt podaje w dokumencie: https://usecryptmessenger.com/plus/wp-content/uploads/2020/11/Licencja-Usecrypt-Messenger.pdf Jednocześnie Signal bazuje na kodeku dźwiękowym webRTC firmy Google, wykorzystanym przez NSO, producenta Pegasusa do zainfekowania telefonu, opisanym przez Financial Times: https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab Usecrypt stworzył własny serwer dźwiękowy, co stanowi game-changer i odporność na ten wektor ataku.

4	NIEPRAWDZIWA INFORMACJA W ARTYKULE: W tzw. międzyczasie **część polskich specjalistów zajmujących się bezpieczeństwem skrytykowała niektóre elementy tej aplikacji, wskazując na zaskakujące niedoróbki.**	**Nieprawdą jest, że powstał więcej niż 1 materiał dot. rzekomych „niedoróbek”** w aplikacji Usecrypt. Link: https://informatykzakladowy.pl/bo-do-komunikatora-trzeba-dwojga/ **Nieprawdą jest byli to specjaliści zajmujący się bezpieczeństwem** oraz **że zostały wskazane jakiekolwiek niedoróbki** aplikacji Usecrypt. **Tekst Informatyka Zakładowego był manipulacją**, nie dotyczył aplikacji Usecrypt lecz innej aplikacji i został sprostowany: https://informatykzakladowy.pl/sprostowanie/ Dodatkowa opinia w tym zakresie została przekazana Redakcji. https://usecryptmessenger.com/plus/opinia.pdf
5	NIEPRAWDZIWA INFORMACJA W ARTYKULE: Skrytykowano też **tezy z ich agresywnego przekazu dotyczące konkurencji, jako w wielu miejscach naciągane.**	Usecrypt wskazywał abuzywn polityk prywatności innych komunikatorów, zostały potwierdzone poprzez ich zmiany i/lub zapowiedź ich zmian m.in. przez WhatsApp: https://www.rmf24.pl/fakty/swiat/news-nowa-polityka-prywatnosci-whatsappa-zaklada-przekazywanie-da,nId,4990620 Również zastrzeżenia co do niejasności źródeł finansowania Signala oraz braku jego pełnego bezpieczeństwa zostały ostatnio potwierdzone, poprzez następuje fakty: Link do informacji o sponsorowaniu Signala przez fundusz rządu USA: https://www.google.pl/amp/s/www.brecorder.com/news/amp/40058048 Informacja firmy Cellebrite, o uzyskaniu dostępu do bazy aplikacji Signal na telefonie: https://www.bbc.com/news/technology-55412230 Film BBC wraz z Privacy International (w mailu)

6	NIEPRAWDZIWA INFORMACJA W ARTYKULE: W reklamie pada parę „buzzwordów” wykorzystujących nośność słowa Mosad i wizerunek Izreala, jako państwa wybitnie dbającego o bezpieczeństwo. **Jednocześnie tych rewelacji nie ma za bardzo gdzie zweryfikować.** **Rekomendacja z Izraela nie została wrzucona na stronę www komunikatora**, nie znalazłem tam nawet najmniejszej wzmianki o niej (a są wspomniani np. WAT czy Dell).	Mimo, iż nie istnieje żaden obowiązek umieszczania tego typu materiałów publicznie Spółka przekazała do wglądu dla Redakcji m.in. następujące dokumenty: - Zgodę Ministerstwa Obrony Narodowej Izraela - List atestacyjny izraelskiej firmy, której zespół związany jest z najbardziej elitarnymi jednostkami cyber w Izraelu - Raport autorstwa izraelskiego duetu - Oded Vanunu i Roman Zaikin, najbardziej poważanego zespół na Świecie badającego bezpieczeństwo komunikatorów
7	NIEPRAWDZIWA INFORMACJA W ARTYKULE: Nie znalazłem też żadnego opisu, w jaki sposób aplikacja miałaby wykrywać obecność Pegasusa, co jest jednym z głównych marketingowych „haczyków” **w tej reklamie.**	Usecrypt złożył 4 wnioski patentowe i uzyskał ochronę „dniem pierwszeństwa” potwierdzając unikalność własnych rozwiązań, dotyczących zabezpieczenia aparatu, czego kompletnie nie posiada Signal, ani żaden inny komunikator: 4. Kontrola Bezpieczeństwa 5. Enter code wraz szyfrowaniem bazy aplikacji na telefonie 6. Panic code Jednocześnie Signal bazuje na kodeku dźwiękowym webRTC firmy Google, który stał się wektorem ataku wykorzystanym przez NSO, producenta Pegasusa, opisanym przez Financial Times: https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab Usecrypt storzył własny serwer dźwiękowy i kodek, co stanowi game-changer w tym wektorze ataku.

8

NIEPRAWDZIWA INFORMACJA W ARTYKULE:

Pozostaje jednak pytanie, czy tak **cepeliowy sposób** jest odpowiednią formą promowania produktu, mającego być świętym Grallem wśród komunikatorów zapewniających bezpieczeństwo naszych rozmów?

Z tego wszystkiego aż sprawdziłem co podaje Google Play i App Store na temat ilości ściągniętych aplikacji oraz opinii użytkowników i jak na komunikator wygląda to słabo.

Subiektywna ocena obraża naszych użytkowników oraz akcjonariuszy.

Aplikacja Usecrypt Messenger jest numerem 1 na AppStore. Liczba ściągniętych aplikacji przez Google przekracza 100.000.