aut. Sylwia Gliwa 07.11.2019

RANSOMWARE: „NAZYWAM SIĘ TRUMP, DONALD TRUMP”

W cyfrowym świecie nie liczą się posągi, pomniki czy ulice nazwane twoim imieniem. Liczy się to czy twoje nazwisko jest na tyle znane, że może posłużyć jako wabik. Swoim cyfrowym śladem w hakerskim świecie może pochwalić się m.in. Donald Trump, którego imieniem nazwano ….ransomware.

Nie tylko Donalda Trumpa spotkał ten niewątpliwy zaszczyt, złośliwego oprogramowania nazwanego swoim imieniem doczekał się również Barack Obama, Hillary Clinton, Władimir Putin czy Kim Jong Un. Cyberprzestępcy wykorzystują wizerunek prezydenta Trumpa, jak i innych prezydentów do oszukiwania ofiar i pozyskiwania środków finansowych. Do swoich działań wykorzystują ataki ransomware, programy do blokowania ekranu i trojany.

„Istnieje szeroki wachlarz zagrożeń, który przeciwnicy są gotowi wykorzystywać za pomocą wszelkich niezbędnych środków, w tym wykorzystując motywy i podteksty” – stwierdzili badacze z Cisco Talos Intelligence Group, którzy zajęli się analizą zagrożenia.

Mechanizm działania jest bardzo prosty. Hakerzy wykorzystują do przyciągnięcia uwagi ofiar w przesyłanych e-mailach lub załącznikach informacje wspominających światowych liderów. Z przebadanych przez Cisco Talos Intelligence Group oprogramowanie pokazało, że motyw wykorzystujący wizerunek polityków jest wykorzystywany nawet przy fałszywym oprogramowaniu ransomware i programów blokujących ekran. Przeanalizowane oprogramowanie niekoniecznie szyfrowały dane, ale jak wskazują eksperci, doprowadzały ofiary do przekonania, że ich dane mogły zostać utracone i tym samym próbowano przekonać ich do przekazania środków finansowych.

„Uderzyła nas różnorodność złośliwego oprogramowania, od ransomware i programów do blokowania ekranu, po trojany reklamowe i trojany dostępu zdalnego oraz wszystko inne” - konkludowali eksperci Cisco Talos Intelligence Group. „Niezależnie od tego, co zaczęło się jako zwykłe zadanie analizy kampanii z spamem, pozwoliło nam znaleźć setki politycznie naładowanych programów, które przynajmniej wskazywały na złośliwe możliwości, nawet jeśli ostatecznie nie były” – czytamy w analizie ekspertów. Wynik badań nie wskazały możliwego pochodzenia badanego złośliwego oprogramowania.