**Trendy cyberzagrożeń w pierwszej połowie 2016 roku**

**Świat malware wciąż rozwija się szybko i dynamicznie. Codziennie pojawiają się nowe wersje szkodliwego oprogramowania, które napędzają zabawę w kotka i myszkę pomiędzy napastnikami a obrońcami. Potęgę zagrożeń doskonale pokazują statystyki – na świecie co 4 sekundy dochodzi do pobrania nieznanych, zarażonych plików, natomiast co 5 sekund użytkownicy wchodzą na zarażone strony WWW.**

Firma Check Point w ostatnim czasie opublikowała raport nt. [globalnych i regionalnych trendów najbardziej pożądanych malware](http://blog.checkpoint.com/wp-content/uploads/2016/10/H1_Malware_Report_161028v2.pdf), który pozwala spojrzeć na krajobraz szkodliwego oprogramowania w trzech czołowych kategoriach – ransomware, bankowości i mobile’u. Raport bazuje na danych z ThreatCloud World Cyber [Threat Map](https://threatmap.checkpoint.com/ThreatPortal/livemap.html), zgromadzonych w okresie od stycznia do czerwca 2016 roku.

Bez wątpienia rok 2016 przejdzie do historii jako przełomowy rok dla ransomware, które konsekwentnie pojawiało się w mediach w ostatnich miesiącach. I to nie bez przyczyny – ataki rosły w ilości, różnorodności, wydajności oraz stopniu wyrafinowania! Ciągły wzrost powszechności ransomware wyraźnie wskazuje na skuteczność tego typu działań. Firmy często decydują się zapłacić okup hakerom, obawiając się utraty ważnych danych. To czyni z całego procederu atrakcyjny i lukratywny biznes.

Napastnicy coraz powszechniej używają tzw. Exploit kitów do rozprzestrzeniania złośliwego oprogramowania. Zestawy te, mające niepokojący wskaźnik skuteczności, wykorzystują luki w przeglądarkach czy systemach operacyjnych do instalacji złośliwego oprogramowania bez zgody oraz wiedzy użytkownika. Jak pokazuje przypadek Nuclear Exploit Kit, może to być niezwykle dochodowy biznes dla deweloperów, którzy wynajmują swoje zestawy napastnikom na całym świecie. W bieżącym roku mogliśmy dostrzec wzrosty na scenie exploit kitów – zarówno Angler, Nuclear odnoszą coraz większą popularność, jak również Neutrino czy Rig, wykorzystywane w ostatniej kampanii hakerskiej Cerber

W 2016 roku nowa forma malware pojawiała się w świecie mobilnych technologii – są nią botnety. Botnet to w skrócie grupa urządzeń (PC, laptopy, telefony komórkowe) kontrolowana przez hakerów bez wiedzy właściciela. Im większy jest sieć, tym większe są jej możliwości. Zidentyfikowane przez Check Pointa botnety – takie jak Viking Horde czy DressCode – potrafią zinfiltrować Google Play i wykorzystać setki tysięcy użytkowników.

Jak do tej pory mobilne botnety były wykorzystywane głównie do generowania fałszywego ruchu i klików reklam. Jednakże, mogą być również użyte do osiągnięcia celów czysto destrukcyjnych takich jak ataki DDoS, które mogą mieć niszczycielski wpływ na różnego rodzaju organizacje



Pierwsza połowa 2016 roku pokazuje naturę dzisiejszego krajobrazu zagrożeń cybernetycznych. Wiele starych zagrożeń wciąż pozostaje widocznych i aktywnych, natomiast nowe szturmem starają się zdobyć świat. Jak się okazuje nieliczna część rodzin malware odpowiada za większość skutecznych ataków na świecie – jedynie 10 z ponad 2000 rodzin odpowiada za ponad 50% wszystkich ataków!

Jak można dostrzec – większość cyberzagrożeń ma charakter globalny i ponadregionalny, a czołowe z nich pojawiają się we wszystkich trzech regionach. W każdym z regionów dominuje malware skupiony na bankowości. W EMEA (Europa, Środkowy Wschód i Afryka) coraz większą rolę odgrywa ransomware (24% wszystkich malware) i zgodnie z prognozami firmy Check Point rynek tego typu malware będzie się wciąż dynamicznie rozwijał.

