Cyberdefence 24

aut. Tomasz Fastyn 14.02.2017

ENISA: RANSOMWARE CORAZ WIĘKSZYM ZAGROŻENIEM

Ostatni raport Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA) pokazuje, że nadal największym zagrożeniem pozostaje złośliwe oprogramowanie i ataki na strony internetowe. W ciągu roku zwiększyły się straty spowodowane przez działania DDoS-ów, phishingu, spamu i oprogramowania wymuszającego okup.

ENISA w podsumowaniu zagrożeń cybernetycznych w 2016 roku zauważa, że najszybciej rozwijającą się dziedziną przestępstw były kampanie ransomware. Mimo większego zagrożenia, oprogramowanie wymuszające okup nadal nie jest najpowszechniejszym narzędziem hakerów. Niezmiennie od kilku lat, na pierwszym miejscu, według raportu *Threat Landscape 2016*, znajdziemy złośliwe oprogramowanie. Na kolejnych pozycjach mamy natomiast ataki na strony i aplikacje internetowe.

Nowość w rankingu zagrożeń pojawia się dopiero na miejscu 4., gdzie do tej pory można było odnaleźć botnety. Jednak w 2016 roku, według agencji ENISA to ataki DDoS stanowiły większe zagrożenie. Komputery zombie skupione w sieciach (tzw. botnety) w zeszłym roku przegrały rywalizacje z internetem rzeczy, który pozwolił na lepsze wykorzystanie sieci, wyłączając nawet serwer DNS należący do DNY.

Czytaj też: USA: Wzrasta ochrona korespondencji mailowej obywateli

O dwa oczka w górę w rankingu skoczył także phishing i spam zajmujące kolejno 6. i 7 miejsce. Wszystkich, których śledzili zmiany rynku w zeszłym roku, nie zaskoczy wysoka pozycja oprogramowania wymuszającego okup na miejscu 8. W zeszłorocznym raporcie zajmowało ono dół stawki, dostając od autorów raportu przedostatnią, 14 lokatę.

ENISA w swoim raporcie porusza także temat zmian w postrzeganiu całego krajobrazu cyberprzestępstw, który dla wielu hakerów czy nawet firm, stał się nowym rynkiem inwestycyjnym. Oprócz wynajmowania hakerów do wykonywania nielegalnych działań, w zeszłym roku upowszechniły się rozwiązania „crime-as-a-service". Czyli oprogramowania, które przestępcy coraz chętniej udostępniają użytkownikom za odpowiednią opłatą.

W podziemiu hakerskim pojawiła się także możliwość wynajmowania ransomware dla własnych zysków. Popularne są także inwestycje w konkretne rodziny trojanów, przypominające pakiety akcji. Osoby wspierające rozwój oprogramowania mogą liczyć na dywidendy wypłacane przez twórców. Zwroty z lokowania kapitału w tych rozwiązaniach, został oszacowany na 1400 procent w 2015 roku.