NAJPOPULARNIEJSZE METODY CYBERATAKÓW NA POLSKIE FIRMY I INSTYTUCJE

Specjaliści firmy Fortinet przeprowadzili badanie dotyczące najpopularniejszych metod cyberataków wymierzonych w polskie instytucje oraz przedsiębiorstwa. Jak wynika z analiz, najczęściej wykorzystywanym przez hakerów złośliwym oprogramowaniem szyfrującym pliki dla okupu jest GandCrab.

W drugiej połowie ubiegłego roku odnotowano ponad 1500 przypadków ataków z użyciem różnych wariantów tego robaka. Jednocześnie GandCrab był wówczas najczęściej występującym oprogramowaniem szyfrującym (ransomware) na świecie - odkryto ponad 3 mln ataków z jego wykorzystaniem.

Odnotowano natomiast spadek aktywności wirusa WannaCry, który w 2017 roku sparaliżował na całym świecie wiele instytucji i firm i spowodował straty obecnie szacowane na 8 mld dolarów. W drugiej połowie 2018 r. wypadł z grona najczęściej używanego w Polsce ransomware, na całym świecie zaś zanotowano jedynie 16 tys. przypadków ataków z jego użyciem.

Ransomware, które wystąpiło w omawianym okresie w Polsce, ale nie zostało zauważone w podobnej skali na świecie, to Shade. Wirus ten pojawił się około 2014 roku i w drugiej połowie ubiegłego roku odkryto 228 przypadków jego użycia w atakach na firmy i instytucje. Rozprzestrzenia się przez tzw. malspam, czyli niechcianą korespondencję zawierającą złośliwy załącznik.

Wirus polskiego pochodzenia o nazwie Prosiak zyskał popularność wśród hakerów na całym świecie - w drugiej połowie 2018 r. użyto go prawie 28 mln razy. W Polsce było ponad 270 tys. ataków z jego użyciem. Prosiak to narzędzie, które umożliwia cyberprzestępcom zdobycie "tylnej furtki" do obranego za cel systemu bądź sieci komputerowej.

Eksperci Fortinetu ostrzegli w swoim raporcie przed coraz częstszym wykorzystywaniu przez hakerów luk w zabezpieczeniach legalnego oprogramowania popularnego w firmach i instytucjach, takiego jak Adobe Reader i Acrobat a także pakiet MS Office. Zdaniem specjalistów liczba aktywnych prób wykorzystania luk tego ostatniego produktu sięgnęła w omawianym okresie poziomu ponad 41 tys. przypadków.

Firma zauważa, że istotnym zagrożeniem pozostają botnety, które są sieciami zainfekowanych przez złośliwe oprogramowanie komputerów lub urządzeń tzw. internetu rzeczy (IoT). Z ich użyciem cyberprzestępcy mogą rozpowszechniać złośliwe oprogramowanie, rozsyłać spam lub przeprowadzać ataki zmasowanej odmowy dostępu do usług (DDoS). Według specjalistów Fortinetu obecnie dwa

najpopularniejsze botnety w Polsce to H-worm i Zeroaccess. Łącznie odnotowano ponad 6 mln przypadków aktywności każdego z nich.

Badanie firmy Fortinet zostało przeprowadzone z użyciem czujników laboratorium FortiGuard rozmieszczonych na terenie Polski. Dane zebrano w okresie od 1 czerwca do 31 grudnia 2019 r.

SZP/PAP