NOWE CYBERWYZWANIA SEKTORA FINANSOWEGO

Tylko od sierpnia do października 2018 roku ze sklepu Google Play usunięto 29 fałszywych aplikacji bankowych, które zawierały trojany. Nastąpiło to dopiero po tym, jak zostały zainstalowane przez ponad 30 tys. użytkowników. Złośliwe oprogramowanie m.in. wykrada dane logowania, wiadomości SMS czy listy kontaktów. Jeden Android.banker.A2f8a zbierał je z ponad 200 różnych aplikacji bankowych. Jakie kolejne wyzwania przyniesie branży finansowej nadchodzący rok?

Urządzenia mobilne na celowniku

Ochrona przed złośliwym oprogramowaniem jest coraz trudniejsza, ponieważ nie zawsze pochodzi ono z podejrzanych i niesprawdzonych źródeł. Ataki na urządzenia i aplikacje mobilne umożliwiają hakerom nie tylko kradzież danych, ale też przechwytywanie ruchu sieciowego przesyłanego pomiędzy użytkownikiem a jego bankiem czy monitorowanie transakcji finansowych dokonywanych przez internet. Zagrożeni są nie tylko konsumenci, ale i firmy – zainfekowane urządzenia mogą stać się bramą dostępu do sieci całej organizacji.

Szyfrowanie i botnety zagrożeniem dla sieci

Według danych z laboratorium FortiGuard Labs firmy Fortinet, już 72% ruchu sieciowego jest zaszyfrowane (w roku 2017 było to 55%). Pozwala to na ochronę wrażliwych danych i transakcji. Szyfrowanie może jednak też stanowić czynnik osłabiający wydajność zapór sieciowych i systemów wykrywania intruzów (IPS), ponieważ ogranicza możliwość szybkiego sprawdzania danych. W rezultacie coraz większy odsetek ruchu sieciowego może być analizowany pod kątem złośliwej aktywności jedynie pobieżnie, aby nie spowalniać ważnych transakcji finansowych. Sytuacji nie poprawia także zaniedbywanie przez wiele organizacji kwestii aktualizowania wszystkich urządzeń i systemów. Niezałatane luki wykorzystywane są m.in. przez coraz bardziej inteligentne, złożone i trudne do wykrycia botnety. Mogą one pozostawać w sieci organizacji średnio przez ponad 10 dni (w 2017 roku było to więcej niż 7 dni). Wiele botów przerywa przy tym swoje działanie po wykryciu i wznawia je dopiero, gdy przywrócone zostaną standardowe operacje systemu. Jedynym sposobem jest wtedy odnalezienie i usunięcie „pacjenta zero”.

Nowe wyzwania wymuszają zmiany

Cyberataki są przeprowadzane w coraz szybszym tempie, a to oznacza mniej czasu na prewencję, wykrywanie i minimalizowanie ich skutków. Błyskawiczna reakcja staje się kluczowa, dlatego organizacje powinny zmienić swoją politykę cyberbezpieczeństwa. Konieczne jest odejście od rozwiązań z zakresu ochrony punktowej, manualnego zarządzania bezpieczeństwem czy ochrony jako

reakcji na zagrożenie, które już wystąpiło.

Strategia powinna integrować wszystkie elementy systemu zabezpieczeń oraz zbierać i porównywać informacje o zagrożeniach. Wzrośnie również waga kontroli dostępu do sieci. Identyfikacja i nadzorowanie wszystkich urządzeń, także mobilnych oraz z zakresu IoT, umożliwi wczesne wykrywanie niestandardowej i podejrzanej aktywności.

Aby chronić klientów i transakcje, niektóre duże banki wprowadziły do swoich aplikacji także zabezpieczenia biometryczne. Nie wszystkie podmioty mają taką możliwość, jednak każdy powinien przynajmniej regularnie skanować sieć pod kątem fałszywych aplikacji, a po ich znalezieniu ostrzegać klientów i nakłaniać witryny czy sklepy do ich usuwania.

– *Warto również pamiętać o mechanizmach ochrony i edukowania samych konsumentów. Wielu cyberprzestępców wykorzystuje socjotechniki do wyłudzania danych, dlatego organizacje finansowe powinny przypominać klientom, o jakie dane może prosić oryginalna aplikacja lub konsultant, a o jakie nie* – mówi Wojciech Ciesielski, menedżer Fortinet ds. sektora finansowego.

Źródło: Fortinet