W 2018 r. trojany atakowały 16 proc. częściej

ID artykułu: 56946 / 2264

URL: http://www.publikuj.org/56946

W 2018 roku 889 452 użytkowników rozwiązań Kaspersky Lab było atakowanych przez trojany bankowe, co stanowi wzrost o 15, 9% w porównaniu z 2017 r., gdy liczba ta wynosiła 767 000.

Według przeprowadzonej przez Kaspersky Lab analizy krajobrazu zagrożeń finansowych za wzrost ten częściowo odpowiada wzmożona aktywność jednego trojana bankowego.

Ataki przy użyciu trojanów bankowych, tzw. bankerów, należą do najpopularniejszych wśród cyberprzestępców, ponieważ są bezpośrednio zorientowane na korzyści finansowe. Tego rodzaju szkodliwe oprogramowanie kradnie dane uwierzytelniające do systemów płatności elektronicznych oraz systemów bankowości online, przechwytując kody jednorazowe, a następnie wysyłając te dane przestępcom, którzy stoją za danym trojanem.

Spośród 889 452 zaatakowanych użytkowników niemal 25% stanowiły firmy odsetek ten utrzymywał się na dość stałym poziomie przez ostatnie trzy lata. Według ekspertów z Kaspersky Lab przyczyna tego stanu rzeczy jest jasna: podczas gdy ataki na klientów indywidualnych zapewnią jedynie dostęp do kont bankowości lub systemów płatniczych, udane kampanie wymierzone w pracowników mogą również zapewnić taki dostęp do firmowych środków finansowych.

Z danych wynika również, że Rosja stała się najczęściej atakowanym państwem w 2018 r. ponad 22% użytkowników zaatakowanych bankowym szkodliwym oprogramowaniem na całym świecie znajdowało się właśnie w Rosji. Na drugim miejscu znalazły się Niemcy (z udziałem wynoszącym ponad 20%), a na trzecim Indie (niemal 4%).

Jeśli chodzi o konsumentów, można powiedzieć, że rok 2018 nie przyniósł im dużego wytchnienia od zagrożeń finansowych. Z naszych danych wynika, że niesławne bankery nadal istnieją, zwiększając liczbę swoich ataków i polując na pieniądze. Szczególnie interesujący był trojan bankowy RTM, którego lawinowy wzrost odpowiadał za skok liczby takich szkodników w 2018 r. Dlatego zalecamy użytkownikom zachowanie ostrożności podczas przeprowadzania operacji finansowych online ze swoich komputerów osobistych. Pozostawiając komputer bez ochrony, nie doceniasz profesjonalizmu współczesnych cyberprzestępców powiedział Oleg Kupriejew, ekspert ds. cyberbezpieczeństwa, Kaspersky Lab.

Główne ustalenia przedstawione w raporcie Kaspersky Lab

1. Phishing

W 2018 r. udział phishingu finansowego zmniejszył się z 53, 8% do 44, 7% wszystkich wykrytych ataków phishingowych, ale nadal stanowił niemal połowę wykrytych zagrożeń tego typu.

Mniej więcej jedna na pięć prób załadowania strony phishingowej, która została zablokowana przez produkty firmy Kaspersky Lab, dotyczyła phishingu bankowego.

W 2018 roku udział ataków phishingowych związanych z systemami płatniczymi oraz sklepami internetowymi wynosił odpowiednio niemal 14% i 8, 9%. To nieco mniej niż w 2017 r.

Wzrósł nieco udział phishingu finansowego napotykanego przez użytkowników komputerów Mac który w efekcie stanowił 57, 6% wszystkich ataków phishingowych wymierzonych w platformę macOS.

2. Szkodliwe oprogramowanie bankowe:

W 2018 r. liczba użytkowników zaatakowanych przez trojany bankowe wynosiła 889 452 co stanowi wzrost o 15, 9% w porównaniu z 767 072 atakami w 2017 r.

24, 1% użytkowników zaatakowanych przy użyciu bankowego szkodliwego oprogramowania stanowiło użytkowników korporacyjnych.

Najczęściej atakowani przez szkodliwe oprogramowanie bankowe byli użytkownicy w Rosji, Niemczech, Indiach, Wietnamie, we Włoszech, Stanach Zjednoczonych oraz Chinach.

Jeśli chodzi o najbardziej rozpowszechnione rodziny szkodliwego oprogramowania bankowego, wciąż dominuje Zbot oraz Gozi (ponad 26% i 20% zaatakowanych użytkowników), podczas gdy na kolejnym miejscu plasuje się SpyEye (15, 6%).

3. Szkodliwe oprogramowanie bankowe dla systemu Android:

W 2018 r. liczba użytkowników, którzy zetknęli się ze szkodliwym oprogramowaniem bankowym dla systemu Android, zwiększyła się ponad trzykrotnie do 1 799 891 na całym świecie.

Za ataki na ogromną większość użytkowników (około 85%) odpowiadały tylko trzy rodziny szkodliwego oprogramowania bankowego.

Rosja, Afryka Południowa oraz Stany Zjednoczone stanowiły państwa o najwyższym odsetku użytkowników atakowanych przez szkodliwe oprogramowanie bankowe dla system Android.

Porady bezpieczeństwa

W celu zabezpieczenia się przed phishingiem finansowym eksperci z Kaspersky Lab zalecają użytkownikom prywatnym podjęcie następujących działań:

Strony internetowe mogą stanowić dla cyberprzestępców przykrywkę dla przechwytywania Twoich danych. Aby poufne dane nie wpadły w niepowołane ręce, jeśli jakaś strona wydaje się podejrzana lub jest nieznana, nie podawaj na niej swoich danych dotyczących karty kredytowej ani nie dokonuj zakupów.

Wyspecjalizowane rozwiązanie zabezpieczające na Twoim urządzeniu, z wbudowanymi odpowiednimi funkcjami, stworzy bezpieczne środowisko dla wszystkich transakcji finansowych, pomagając w zapobieganiu oszustwom finansowym. Technologia Bezpieczne pieniądze firmy Kaspersky Lab powstała z myślą o zapewnieniu użytkownikom takiego poziomu ochrony, jak również spokoju umysłu. Stosuj niezawodne rozwiązanie zabezpieczające, takie jak Kaspersky Total Security, zapewniające wszechstronną ochronę przed szerokim wachlarzem zagrożeń.

Aby zapewnić bezpieczeństwo swoim danym uwierzytelniającym, należy stosować ten sam stopień czujności i ochrony wobec wszystkich swoich urządzeń zarówno komputerów stacjonarnych, laptopów jak i urządzeń mobilnych. Działalność cyberprzestępców nie ma granic, dlatego ochrona musi być równie wszechstronna w celu zminimalizowania ryzyka, że Twoje informacje wpadną w niepowołane ręce. Do przechowywania cennych danych cyfrowych wykorzystuj niezawodne rozwiązanie zabezpieczające, takiego jak Kaspersky Password Manager.

Dla firm eksperci z Kaspersky Lab przygotowali następujące wskazówki:

Zainwestuj w regularne szkolenia dla pracowników ukierunkowane na zwiększenie świadomości w zakresie

cyberbezpieczeństwa, podczas których nauczą się, aby nie klikać odsyłaczy ani nie otwierać załączników otrzymanych z niezaufanych źródeł. Przeprowadź symulacje ataków phishingowych, aby mieć pewność, że pracownicy potrafią rozpoznać wiadomości phishingowe.

Wykorzystuj zaawansowane technologie wykrywania i reagowania, takie jak Kaspersky Endpoint Detection and Response, wchodzące w skład rozwiązania Threat Management and Defense. Umożliwia ono wykrywanie nawet nieznanego szkodliwego oprogramowania bankowego i zapewnia zespołom odpowiedzialnym za operacje bezpieczeństwa pełną widoczność swojej sieci oraz automatyzację reagowania.

Zapewnij swojemu zespołowi z centrum operacji bezpieczeństwa dostęp do analizy zagrożeń, tak aby był na bieżąco z najnowszymi taktykami i narzędziami wykorzystywanymi przez cyberprzestępców.

Więcej informacji na temat phishingu finansowego znajduje się w pełnym raporcie Kaspersky Lab, dostępnym na stronie https://r.kaspersky.pl/VJKMm span style="font-size: 11.0pt; line-height: 115%; mso-ansi-language: PL; mso-bidi-font-weight: bold;" .

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie https://www.kaspersky.pl/nowosci.

Piotr Kupczyk
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kup czyk@kaspersky.pl
Tel. 34 390 94 00

Aktywacja: 07/03/19 12:59, odsłony: 63