Jak chronić się przed złośliwym oprogramowaniem?

Cyberprzestępcy bawią się z producentami oprogramowania i z klientami bankowości internetowej w kotka i myszkę. Wymyślają coraz bardziej wyszukane sposoby na zainfekowanie komputerów i urządzeń mobilnych.

Mają nadzieję, że złapiemy się w pułapkę, a oni dostaną się do naszych pieniędzy dzięki pomocy złośliwego oprogramowania. Podstawowe zasady dbania o bezpieczeństwo kontaktów online z bankiem trzeba znać jak kolejność liter w alfabecie.

Dla internetowych złodziei łatwiejszym łupem są użytkownicy komputerów, tabletów i smartfonów niż banki czy firmy specjalizujące się w tworzeniu i sprzedaży oprogramowania.

Cyberprzestępcy liczą na brak naszej uwagi i na to, że przez zainfekowanie urządzeń stacjonarnych lub mobilnych złośliwym oprogramowaniem uda im się dostać do naszych danych i w konsekwencji do pieniędzy.

Niektóre sposoby działania hakerów opisaliśmy w poprzednim tekście cyklu Phishing, smishing, vishing, czyli jak oszuści wykradają poufne dane.

W Polsce (co wyraźnie zaznaczyli analitycy Narodowego Banku Polskiego w opracowaniu „Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2017 r.") systematycznie rośnie powszechność i wartość obrotu bezgotówkowego.

Należymy do krajów o najwyższym użyciu kart zbliżeniowych na świecie. Dynamicznie rozwijają się również płatności mobilne „stając się coraz bardziej powszechne, głównie za sprawą łatwej dostępności do telefonów komórkowych typu smartfon."

Z badań cytowanych w raporcie NBP („Finansowy Barometr ING") wynika również, że dla Polaków płatności bezgotówkowe są bardziej bezpieczne niż gotówkowe. Wiele osób uważa, iż wadą noszenia ze sobą gotówki jest to, że stosunkowo łatwo ją stracić.

Zaś płatności bezgotówkowe mają – zdaniem respondentów – więcej zabezpieczeń przed nieuprawnionym użyciem (pin, kod, hasło lub odcisk palca). Autorzy badania przypominają jednak, iż w przypadku kradzieży gotówki szkoda ograniczy się do kwoty, jaką mieliśmy w portmonetce. W przypadku złamania zabezpieczeń internetowych straty mogą być wyższe.

ARC Rynek i Opinia zapytała w listopadzie zeszłego roku o obawy związane z korzystaniem z nowoczesnych finansowych technologii. Badanie przeprowadzono dla Biura Informacji Kredytowej.

Sześciu na dziesięciu ankietowanych obawia się możliwości użycia złośliwego oprogramowania komputerowego w celu uzyskania ich danych. Najbardziej ostrożne są osoby w wieku 55+. Młodsi mają mniej obaw, co być może wynika z ich lepszej umiejętności poruszania się w wirtualnym świecie.

Złośliwe oprogramowanie (w zależności od sposobu atakowania infrastruktury określane jako wirusy, robaki, programy szpiegujące, konie trojańskie) to specjalne oprogramowanie stworzone po to, by zakłócić pracę komputera.

Oprogramowanie takie może wykradać informacje poufne, zwolnić działanie komputera lub wysyłać fałszywe e-maile z konta użytkownika, często bez jego wiedzy.

ad

Warto pamiętać, że to my, użytkownicy sprzętu komputerowego, wprowadzamy na urządzenia złośliwe oprogramowanie. Możemy to zrobić, pobierając z internetu bezpłatne programy, które zawierają ukryte złośliwe oprogramowanie; odwiedzając zainfekowane wirusami strony, otwierając załączniki do wiadomości internetowej czy „klikając" na zdjęcia–wirusy wysłane z portali społecznościowych.

Złodzieje stosują coraz bardziej wyrafinowane metody. Ich finezja polega na tym, że coraz skuteczniej podszywają się pod naszych znajomych, firmy, z którymi kooperujemy, banki czy legalne programy. Złośliwe oprogramowanie może być „schowane" w fałszywych komunikatach o błędach lub w wyskakujących okienkach informujących nas o potencjalnych cyberzagrożeniach.

Niekiedy przejmujemy je w postaci „śmiesznych" obrazów i plików audio/wideo. Wirusy mogą być ukryte w pirackim oprogramowaniu i innych plikach dostępnych w sieci.

Przykłady działania złośliwego oprogramowania opisane są między innymi w ostatnim dostępnym raporcie „Krajobraz bezpieczeństwa polskiego internetu w 2016 r." przygotowanym przez CERT Polska. CERT Polska (Computer Emergency Response Team) to zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo użytkowników lub instytucji w internecie.

Działa on od 1996 r. przy NASK (Naukowej i Akademickiej Sieci Komputerowej). Co roku publikuje raport dotyczący cyberbezpieczeństwa. Dwa lata temu CERT Polska zgromadził informacje o 1 694 794 unikalnych adresach IP wykazujących aktywność zombie. Na przykład zauważono odrodzenie trojana bankowego

VBKlip sprzed kilku lat. Tym razem nazwano go „Benio66." Jego celem była podmiana numeru konta bankowego w pamięci przeglądarki. Klienci 12 banków dostali fałszywe wiadomości (maile) z potwierdzeniem transakcji z jednego z polskich banków. „Celem trojana było 12 działających w Polsce banków, aczkolwiek przy pięciu z nich podmiana była zablokowana." – napisano w raporcie CERT Polska.

A na początku roku sam zespół ekspertów przestrzegł przed „złośliwym" oprogramowaniem Malware, który jest wariantem BankBot-ów. Jedną z podstawowych funkcji bota jest wykradanie danych logowania do kont bankowych. Nazwy „złośliwych" aplikacji to: Crypto Monitor; StorySaver oraz Cryptocurrencies Market Prices.

Jak tłumaczą autorzy strony internetowej CERT Polska: „Należy pamiętać o tym, aby nie instalować aplikacji z nieznanych źródeł. Jak się okazało, aplikacje legalne również mogą być niebezpieczne.

Aby się przed tym uchronić, możemy skorzystać z podstawowych mechanizmów bezpieczeństwa systemu Android na przykład zwracać uwagę na listę wymaganych uprawnień, które wyświetlają się przy instalacji aplikacji. Przykładowo, jeżeli aplikacja monitorująca kursy walut prosi o możliwość odczytywania wiadomości SMS, jest spora szansa, że wykorzysta te uprawnienia do wysłania treści wiadomości na zewnętrzny serwer."

Warto więc pamiętać o podstawowych zasadach, które pomogą zminimalizować zagrożenie wynikające z możliwości zainstalowania złośliwego oprogramowania:

1. Instalujmy tylko legalne oprogramowanie i aktualizujmy je oraz system operacyjny komputera. Modernizacja programów często zawiera poprawki, które zwiększają bezpieczeństwo komputera. Niektóre systemy operacyjne są wyposażone w mechanizm automatycznych aktualizacji, dzięki któremu wszelkie uaktualnienia są pobierane samoczynnie tuż po ich udostępnieniu.

2. Rozsądnie i z namysłem klikajmy w linki i pobierajmy załączniki. Ta zasada dotyczy zarówno witryn internetowych, portali społecznościowych, jak i naszej poczty internetowej. Warto zastanowić się nad tym, jakie programy pobieramy z różnych witryn oraz jakie otwieramy załączniki.

3. Szczególnie (na co zwracają uwagę twórcy legalnego oprogramowania) nie ufajmy wyskakującym okienkom z prośbami o pobranie oprogramowania. Na przykład Microsoft przestrzega: „surfując po sieci, możesz natknąć się na witryny, w których pojawiają się wyskakujące okienka z komunikatami o rzekomym zainfekowaniu komputera i propozycją pobrania jakiejś aplikacji mającej zapewnić ochronę. Nie daj się na to nabrać.

Po prostu zamknij wyskakujące okienko, uważając jednocześnie, by nie kliknąć jego zawartości". Uwaga: nie klikamy przycisków „zgadzam się" lub „OK", aby zamknąć okno, które podejrzewamy, że może zawierać program szpiegujący. Zamiast tego kliknijmy czerwony znak „x" w rogu okna lub naciśnijmy klawisze Alt + F4, aby zamknąć to okno.

4. Powinniśmy też uważać w czasie wymieniania plików z innymi użytkownikami. Część witryn, które umożliwiają takie działanie, nie chroni przed złośliwym oprogramowaniem. Złośliwe oprogramowanie może trafić do komputera czy telefonu razem ze ściągniętym filmem czy koncertem. Upewnijmy się, że znamy oprogramowanie spakowane z tymi programami.

5. Zawsze stosujmy programy antywirusowe, jeśli pobieramy pliki z netu. Sprawdźmy, czy nie zainfekowaliśmy urządzenia. Warto regularnie skanować komputer czy telefon, by wykrywać złośliwe oprogramowanie i zapobiegać jego rozprzestrzenianiu się.

6. Jeśli w naszym komputerze jest kilka kont użytkownika, to nie korzystajmy z konta administratora, tylko ze standardowego użytkownika.

7. Gdy korzystamy z urządzeń mobilnych z publicznej sieci Wi-Fi, należy odznaczyć pole „automatycznych połączeń w przyszłości".

W celu sprawdzenia, czy system nie został zainfekowany jakimś złośliwym oprogramowaniem, trzeba uruchamiać regularnie programy skanujące. Producenci programów antywirusowych często na swoich stronach www oferują bezpłatne wersje.