JAKIE CYBERZAGROŻENIA CZYHAJĄ

na polskich użytkowników urządzeń mobilnych?

Łukasz Cepok

Incident Response Manager w Mediarecovery

Zdjęcia: Mediarecovery.

Łukasz Cepok – od początku ścieżki zawodowej związany z IT w organizacjach z sektora finansowego: od młodszego administratora IT i kierownika zespołu IT, przez analityka L1, do eksperta Incident Response. Od kilku lat zaangażowany w role Cyber Threat Intelligence. Uważa, że te dwa procesy nie mogą istnieć oddzielnie i muszą się wzajemnie uzupełniać. Analityk złośliwego oprogramowania na urządzenia mobilne. Lubi dzielić się wiedzą w rolach wykładowcy lub prelegenta. W życiu prywatnym również angażuje się w rozwiązywanie incydentów jako strażak ochotnik.

Polska przestrzeń cyfrowa nie jest bezpieczną przystanią, to front ciągłej walki o dane i pieniądze użytkowników. Na cyberzagrożenia narażone są także urządzenia mobilne – smartfony, które nosimy w kieszeniach i często uważamy je za bezpieczniejsze od komputerów. Wiele osób jest o tym przekonanych, ponieważ ataki na urządzenia mobilne nie są tak spektakularne i nie przebijają się do mediów głównego nurtu. A prawda jest zgoła inna.

Urządzenia mobilne już dawno zastąpiły nam komputery w większości czynności codziennych. Wykorzystujemy je do wielu aktywności: realizujemy przez nie zakupy, płacimy rachunki, obsługujemy pocztę elektroniczną oraz korespondencję z urzędami, wykorzystujemy do komunikacji z innymi użytkownikami. Okazuje się zatem, że telefony, zwane również smartfonami, czy szerzej – urządzenia mobilne – w obecnych czasach służą za banki informacji o nas, przechowujemy na nich informacje, dokumenty, zdjęcia i inne treści cyfrowe. Tymi wszystkimi danymi zainteresowane są różne grupy przestępcze, każda z nich będzie chciała wykorzystać je na swój sposób, ale cel jest jeden: monetyzacja ataku, czyli przestępcom atak musi się po prostu opłacać.

Co istotne z punktu widzenia cyberbezpieczeństwa, zagrożenia znane z komputerów można praktycznie w pełni odwzorować na urządzeniach mobilnych, a więc istnieją np. phishing, złośliwe oprogramowanie, oszustwa itp.

Warto zatem dowiedzieć się, jakie cyberzagrożenia czyhają na użytkowników. I tak, na przykład w ramach złośliwego oprogramowania możemy zetknąć się z nw. klasami zagrożeń.

Spyware/stealer

Oprogramowanie, które ma za zadanie wykradać informacje użytkownika i o użytkowniku, które następnie będą wykorzystywane w dalszych etapach ataków lub odsprzedawane innym grupom wyspecjalizowanym w konkretnych atakach i zainteresowanych tego typu danymi.

Adware

Jest oprogramowaniem, którego głównym celem jest monetyzowanie oszustw na sieciach reklamowych. Z pozoru niewinne aplikacje serwują użytkownikowi setki niewidocznych reklam, co powoduje zużycie zasobów baterii, sieć reklamowa odbiera informację o tym, że użytkownik zobaczył reklamy i wypłaca autorowi aplikacji prowizje i nagrody za wygenerowane obejrzenia.

Ransomware

To zagrożenie kojarzy nam się jednoznacznie z atakami na komputery i sieci firmowe. Jednak przestępcy od dawna już eksperymentują z tego typu oprogramowaniem w atakach na telefony. Co prawda nie jest ono jeszcze w pełni skuteczne, co wynika bezpośrednio z architektury systemów operacyjnych urządzeń mobilnych, ale to kwestia czasu, aż zostanie odpowiednio rozwinięte.

WebAPK

Technologia do instalowania plików do aplikacji internetowych wykorzystywana do przeprowadzania ataków phishingowych lub legendowania oszustw, zagrożenie to zostało odkryte w lipcu 2023 r. przez CSIRT KNF.

NFC Relay

Początkowo uznany za atak możliwy tylko w warunkach laboratoryjnych, pokazuje, że przestępcy potrafią zaadaptować skomplikowane mechanizmy sieci płatniczych do monetyzowania ataków.

Ostatnim wartym nadmienienia zagrożeniem są **trojany** – można je podzielić na kilka grup: bankowe, RAT i te najbardziej zaawansowane jak oprogramowanie klasy Pegasus.
To właśnie trojany bankowe były w Polsce wykorzystywane przez przestępców od 2017 r. i były najpopularniejszym zagrożeniem aż do 2022 r.
Warto zauważyć, że obecnie zagrożenia mobilne działają w modelu MaaS (*Malware as a Service*), czyli oprogramowanie do wynajęcia w modelu subskrypcji miesięcznej. Mamy tu zatem tak naprawdę dwie grupy przestępcze: developerów, którzy tworzą takie oprogramowanie, i operatorów, którzy je wynajmują. Ceny takiego oprogramowania na forach przestępczych wahają się od 1000 do 5000 $. Więc tak naprawdę udany atak na jedną lub dwie ofiary spłaca miesięczną inwestycję. Analizy kampanii wykazywały ponadto, że wśród operatorów znajdowały się osoby, których natywnym językiem był język polski, co sugeruje, że były to rodzime grupy przestępcze. Polska ze swoją wysoką adaptacją nowych technologii jako środków płatności, ale również ze społeczeństwem, które bardzo szybko przystosowuje się do rozwiązań fintechowych i jest coraz bardziej „smart", stanowi swego rodzaju poligon doświadczalny dla przestępców.
Można tutaj przytoczyć przykład, kiedy specjaliści od cyberbezpieczeństwa obserwowali ogłoszenia promujące nową rodzinę złośliwego oprogramowania i jeszcze tego samego lub następnego dnia kampania wykorzystująca tego trojana była dystrybuowana do polskich użytkowników. Schemat całego ataku był dosyć prosty, a w dodatku powtarzalny i mimo wysiłków zespołów bezpieczeństwa, czy to po stronie banków, czy CSIRT-ów poziomu krajowego i sektorowego włożonych w ostrzeganie użytkowników, zbierał on bardzo wysokie żniwo.
Jak to wyglądało? Zaczynało się od standardowego SMS-a z treścią dotyczącą codziennych spraw: *Twoja paczka nie mogła zostać dostarczona, uzupełnij adres dostawy w nowej aplikacji* (*link do nowej aplikacji*). Ale były również bardziej bezczelne, takie jak kampanie w czasie pandemii koronawirusa, kiedy promowano aplikację do sprawdzenia, czy jest się zakażonym, przez to, że było trzeba zakaszleć do mikrofonu urządzenia mobilnego. Następnie użytkownik pobierał „nową aplikację" i wtedy pojawiał się „problem w działaniu". Taki komunikat legendował żądania oprogramowania dotyczące wysokich uprawnień, które rzekomo były potrzebne do prawidłowego działania. Kluczowe dla pełnej realizacji tego ataku było jedno uprawnienie – **ułatwienie dostępu** (ang. *Accessibility Access*). To uprawnienie w telefonach z Androidem ma służyć do ułatwiania obsługi urządzenia osobom z dysfunkcjami. Przestępcy zauważyli, że można to uprawnienie wykorzystać do tego, by system/aplikacja same klikały po ekranie urządzenia (mechanizm miał ułatwić sterowanie urządzeniem osobom np. niewidomym). Dzięki temu mogli nadawać sobie wyższe uprawnienia i dostęp do kolejnych elementów systemu.
Kolejnym etapem ataku było poczekanie, aż użytkownik zaloguje się do bankowości elektronicznej, czasem starano się to przyśpieszyć poprzez wysłanie powiadomienia o treści, która powodowała, że użytkownik logował się

do aplikacji w celu zweryfikowania operacji na koncie (np. uznanie 10 000 zł na konto lub podobny, „kuszący" komunikat). Użytkownik, chcąc to zweryfikować, uruchamiał aplikację bankowości mobilnej. W tym momencie trojan przystępował do właściwego etapu ataku. W ułamku sekundy nad ekranem prawidłowej aplikacji bankowości rysowała się tzw. nakładka (nazywana również *overlay* lub *inject*), było to okienko imitujące ekran logowania do aplikacji bankowej. Użytkownik, działając w emocjach, nawet nie zauważał, że nagle system prosi o pełny login/hasło, a dotychczas był to zawsze PIN, odcisk palca czy inny mechanizm biometrii lub uwierzytelniania. Zmanipulowana ofiara wpisywała zatem swoje pełne poświadczenia. Te automatycznie były wysyłane do atakujących i od razu wykorzystywane w systemach bankowych do realizacji transakcji. Na telefon ofiary przychodził co prawda SMS z kodem lub powiadomienie informujące o nowym logowaniu i kod, który miał potwierdzić, że użytkownik świadomie autoryzuje transakcje. W tym momencie działał jednak już kolejny komponent złośliwego oprogramowania pozwalający przejąć atakującym pełną kontrolę nad wiadomościami i powiadomieniami. Powodowało to, że mimo iż powiadomienie dotarło do urządzenia ofiary, nie wyświetlało się ono użytkownikowi, a SMS-y z banku oznaczane były jako odczytane i przesłane do atakujących.

Co więcej, zależnie od użytej rodziny złośliwego oprogramowania przestępcy byli w stanie utrudnić korzystanie użytkownikowi z telefonu podczas kolejnych faz ataku. Polegało to np. na permanentnym blokowaniu i wygaszaniu ekranu urządzenia, co uniemożliwiało korzystanie z niego. W tym czasie atakujący wyprowadzali środki z konta ofiary do wysokości limitów dziennych lub wyżej, wcześniej modyfikując takie limity. Niejednokrotnie zdarzało się, że atakujący wykorzystywali również uproszczone wnioskowanie o produkty kredytowe w aplikacji i składali wniosek o dodatkowe środki. Bywały przypadki, gdy ofiary były nieświadome ataku przez kilkanaście dni. W końcu okazywało się, że nie są w stanie przeprowadzić operacji z wykorzystaniem karty bankowej i dopiero wtedy, po zalogowaniu do banku, uświadamiali sobie, że przez kilkanaście dni ktoś drenował ich środki finansowe.

Atakujący przeważnie przelewali środki na konta innych ofiar, robiąc z nich tzw. muły finansowe. Z kont tych osób środki były przelewane dalej na giełdy kryptowalutowe lub były wykorzystywane do płacenia za zakupy w sklepach internetowych z elektroniką, czasem w połączeniu z oszustwami, które nazywają się refundami. Polegało to na tym, że później były robione zwroty zakupionych rzeczy lub ich podróbek, co pozwalało odzyskać część zapłaconych pieniędzy za sprzęt. W ten sposób atak był monetyzowany więcej niż jeden raz.

Analiza kodu źródłowego takich aplikacji pozwala na wskazanie pełnych możliwości trojanów bankowych. Wykazała ona, że na celowniku przestępców były nie tylko aplikacje bankowe, ale również użytkowe, np. aplikacje zakupowe, pocztowe, obsługujące programy partnerskie. Powód jest prozaiczny, większość użytkowników wykorzystuje ten sam login, hasło do wielu aplikacji i systemów. Uzyskanie przez atakujących dostępu do mało znaczącej aplikacji mogło im dać znacznie więcej niż celowanie od razu w aplikację bankową.

Można sobie np. wyobrazić sytuację, kiedy atakujący przejąłby dostęp do poczty elektronicznej ofiary. W dzisiejszych czasach dostęp do poczty elektronicznej to jak dostęp do tożsamości cyfrowej. Są tam zapisane informacje nie tylko prywatne, ale również o tym, gdzie dane konto zostało wykorzystane do rejestracji. Znając takie informacje, atakujący może zażądać zmiany hasła i link do zmiany przyjdzie właśnie na tę skrzynkę, do której ma on dostęp. Było to wykorzystywane w scenariuszach z wyłudzeniami kodów BLIK na platformach społecznościowych.

Jakie zatem działania mogą podjąć osoby odpowiedzialne za cyberbezpieczeństwo?

Po pierwsze koniecznie należy zwrócić uwagę, że kluczowe w zachowaniu dowodów do analizy ataku jest nieusuwanie SMS-ów, aplikacji, nieresetowanie urządzenia do stanu fabrycznego. Takie działanie usunie co prawda zagrożenie z urządzenia, ale jednocześnie uniemożliwi analizę. Jednocześnie należy pamiętać o tym, że podjęcie powyższych kroków nie odbierze jednak dostępów do kont, do których atakujący uzyskali już dostęp.

Dokładna analiza kodu źródłowego przeprowadzana przez zespoły bezpieczeństwa lub laboratoria informatyki śledczej wraz z zestawieniem z logami z zainfekowanego urządzenia pozwala w pełni odbudować łańcuch zdarzeń w ataku. Dodatkowo właśnie analiza kodu wskaże pełne funkcjonalności złośliwego oprogramowania i pozwoli na wskazanie ofierze, do czego atakujący miał jeszcze dostęp.

Należy zauważyć, że ilość złośliwego oprogramowania znacząco zmalała w 2022 r., to dlatego że grupy, które zajmowały się jego tworzeniem, były pochodzenia rosyjsko-ukraińskiego i doszło do rozłamów pomiędzy nimi ze względu na toczącą się wojnę, a dodatkowo osoby te zostały zaangażowane w działania w ramach konfliktu zbrojnego.

Nie oznacza to jednak, że zagrożenie całkowicie zniknęło. Obecnie wytwarzanie złośliwego oprogramowania zostało przejęte przez grupy pochodzenia tureckiego i nadal się pojawia, a nowe rodzaje oprogramowania nadal są testowane w Polsce, przeciwko polskim użytkownikom.

Summary

What cyber threats are facing Polish mobile devices users?

The author of this article notes that mobile devices have long since replaced computers in most everyday activities and that a lot of information is stored on them. However, smartphone users are not always aware that various criminal groups are interested in all this data. The goal for criminals is, of course, financial benefit. This article presents the types and methods of operation of cybercriminals, and also provides concise information on how to protect yourself against these types of threats.

Tłumaczenie: Beata Pepłowska