Warszawa, 05-10-2023 r.

RZECZNIK PRAW OBYWATELSKICH

Marcin Wiącek

VII.501.165.2023.KSZ

Pan

Janusz Cieszyński

Minister Cyfryzacji

e-PUAP

Szanowny Panie Ministrze,

cyberataki są jednymi z największych zagrożeń XXI wieku[1] **i jako takie stanowią już dosyć powszechne zjawisko. Nowe metody tych ataków muszą być przedmiotem analizy i refleksji, a także reakcji ze strony właściwych organów**. Cyberprzestępczość wpływa bowiem nie tylko na stabilność instytucji państwa, ale także na system polityczny i gospodarczy, bez względu na to wobec jakich podmiotów jest skierowana. Ochrona cyberprzestrzeni jest i niewątpliwie będzie jednym z najczęściej podejmowanych tematów dotyczących bezpieczeństwa[2]. W badaniach nad cyberprzestrzenią podkreśla się natomiast jej ponadnarodowy charakter[3].

[1] K. Snopkiewicz, *Przegląd zagrożeń w cyberprzestrzeni*, Studia Administracji i Bezpieczeństwa, 9/2020, s. 29-41.

[2] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, Bezpieczeństwo Narodowe, nr 22, II, 2012, s. 125-139.

[3] Z. Chmielewski*, Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, Studia z Polityki Publicznej, nr 2(10)2016, s. 103-128.

Biuro Rzecznika Praw Obywatelskich
al. Solidarności 77
00-090 Warszawa

Tel. centr. (+48 22) 55 17 700
Infolinia obywatelska 800 676 676
biurorzecznika@brpo.gov.pl
bip.brpo.gov.pl

Jedną z najbardziej znanych w Polsce definicji cyberprzestrzeni jest ta pochodząca z Doktryny Cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 r.[4] (dalej jako: Doktryna), określająca cyberprzestrzeń jako *„przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami*". Jak wynika z Doktryny, **działania na rzecz cyberbezpieczeństwa muszą być podejmowane z uwzględnieniem ochrony praw człowieka i obywatela, a także poszanowaniem prawa do wolności słowa oraz prywatności.** Proporcjonalność środków bezpieczeństwa w stosunku do zagrożeń powinna być oparta na efektywnej i wiarygodnej analizie ryzyka[5].

Od pewnego czasu szeroko dyskutowanym problemem dotyczącym cyberprzestępczości[6] jest tzw. *juice jacking*, a mianowicie cyberatak wykorzystywany do atakowania urządzeń uniwersalną magistralą szeregową (USB). Atakowanymi urządzeniami są przede wszystkim telefony komórkowe, tablety i laptopy, zaś do ataku wykorzystuje się port ładowania danego urządzenia. Rozróżnia się dwa rodzaje ataków wykorzystujących metodę *juice jacking* – kradzież danych oraz instalację złośliwego oprogramowania[7]. Ten rodzaj cyberataku w sposób niezwykle głęboki ingeruje w prywatność użytkowników sprzętów, o których mowa powyżej, które miały kontakt z zainfekowanym portem, wobec czego stał się przedmiotem zainteresowania Rzecznika Praw Obywatelskich.

---

[4] Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, 2015 r. (https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf, dostęp 11.09.2023).

[5] Ibidem, s. 7.

[6] Szerzej na temat cyberprzestępczości oraz cyberzagrożeń: M. Konieczny, *Cyberprzestępczość – krótka historia, współczesne oblicza i trudna do przewidzenia przyszłość*, Roczniki Administracji i Prawa 2023, XXIII, z. 1, s. 29-50; D. Skoczylas, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, Prawo w działaniu, Sprawy karne, 53/2023, s. 97-113; K. Bartczak, M. Bodych-Biernacka, *Rodzaje cyberzagrożeń i prawne sposoby im przeciwdziałania w kontekście stosowania cyfrowych platform technologicznych w Polsce i UE*, Przegląd Ogranizacji, Nr 3(974), 2021, s. 39-45; M. Górka, *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa* w: *Cyberbezpieczeństwo wyzwaniem XXI w.*, red. T. Dębowski, Łódź-Wrocław, 2018, s. 31-50.

[7] D. Singh, A. K. Biswal, D. Samanta, D. Singh, H. Lee, *Juice Jacking: Security Issues and Improvements in USB Technology*, Sustainability, 2022; 14(2):939 (https://doi.org/10.3390/su14020939, dostęp 05.09.2023).

Gdy osoba chcąca skorzystać z zainfekowanego portu podłącza swoje urządzenie, hakerzy uzyskują wszystkie dane osobowe bądź infekują urządzenie złośliwym oprogramowaniem. Możliwe jest także kopiowanie danych wrażliwych ze smartfona, tabletu bądź urządzenia komputerowego oraz kradzież tożsamości przy wykorzystaniu takich danych (np. z serwisów bankowych) czy też śledzenie urządzeń.

Jak wynika z analizy przedstawionego powyżej zagadnienia[8] istnieją także sposoby na zeskanowanie telefonu komórkowego w poszukiwaniu konkretnych informacji, szczegółów kont użytkownika, danych związanych z bankowością elektroniczną, w tym m. in. szczegółów dotyczących karty debetowej (kredytowej), a także aplikacji obsługujących przelewy. Dzięki metodom stosowanym przez hakerów – jak wynika z analiz ekspertów – uzyskują oni nazwy użytkownika i hasła w ciągu zaledwie ułamka sekundy. Ponadto w przypadku wariantu polegającego na wgraniu dzięki tej metodzie oprogramowania szpiegującego należy wskazać – co także wynika z analiz ekspertów – że takie oprogramowanie może monitorować zainfekowane urządzenie przez długi czas, może także zamrozić urządzenie i zaszyfrować wszystkie dane uniemożliwiając powtórny dostęp użytkownika do jego danych.

Jakkolwiek trwają badania i prace nad ograniczeniem zagrożeń związanych ze zjawiskiem *juice jacking*, to jednak rozwój złośliwego oprogramowania, a także ostrzeżenia dla użytkowników publicznych portów USB wskazujące na unikanie ich stawia pytania o użyteczność i sens rozbudowywania takich publicznych sieci. Przywołać można przykładowo, wydane przez Federalne Biuro Śledcze, ostrzeżenia[9] dla użytkowników publicznych portów USB informujące o tym, że hakerzy znaleźli sposób na wprowadzenie tam złośliwego oprogramowania oraz oprogramowania

[8] Sh. Sanwal, K. Singh, *Juice Jacking - A type of Cyber Attack, Juice Jacking - A type of Cyber attack,* 2020 Cybernomics, 2(1), s. 25-28 (https://www.cybernomics.in/index.php/cnm/article/view/189/172, dostęp 15.09.2023).

[9] J. Clover, FBI warns against using public USB ports due to malware risk, MacRumors, 10.04.2023 (https://www.macrumors.com/2023/04/10/fbi-malware-public-usb-port-warning/, dostęp 15.09.2023); D. Olszewski, *FBI ostrzega przed publicznymi ładowarkami USB*, ComputerWorld, 12.04.2023 (https://www.computerworld.pl/news/FBI-ostrzega-przed-publicznymi-ladowarkami-USB,445072.html (dostęp 25.09.2023).

monitorującego urządzenia. W ostrzeżeniu wskazano na to, że celowe jest noszenie własnego sprzętu ładującego obsługiwanego przez gniazdka elektryczne[10].

Mimo tego typu ostrzeżeń w przestrzeni publicznej pojawia się coraz więcej takich form wsparcia dla użytkowników, także ze środków publicznych[11].

Mając na uwadze coraz liczniejsze ostrzeżenia przed taką formą cyberataku, chciałbym zwrócić uwagę Pana Ministra na ten problem i jednocześnie uzyskać informację na temat ewentualnych działań podejmowanych przez Ministerstwo Cyfryzacji i rząd w tej kwestii. Szczególną troską Rzecznika Praw Obywatelskich jest kwestia możliwości zainfekowania telefonu użytkownika publicznego portu USB, który w swoim urządzeniu mobilnym posiada rządowe aplikacje – przykładowo mObywatel.

mObywatel 2.0 to aplikacja, którą od dnia 14 lipca bieżącego roku można bezpiecznie i bezpłatnie pobrać na swój smartfon ze sklepu Google Play i App Store. Nowa aplikacja to przede wszystkim asystent obywatela, dzięki któremu załatwianie spraw urzędowych ma być – jak wynika z informacji umieszczonej na stronie internetowej Ministerstwa Cyfryzacji[12] – prostsze i wygodniejsze – bez wychodzenia z domu. Dzięki tej aplikacji możliwe jest korzystanie z dokumentów tożsamości i załatwianie spraw urzędowych. Należy także przypomnieć wcześniejsze informacje dotyczące preinstalacji rządowych aplikacji na wszystkich urządzeniach mobilnych przed ich

[10] Eksperci z ChronPESEL.pl radzili także, aby „*nie podłączać naszych urządzeń do portów USB w miejscach publicznych. Kiedy nie mamy wyjścia i musimy w takim urządzeniu naładować telefon, powinniśmy używać własnego kabla USB - najlepiej takiego, który nie pozwala na przesył danych*" https://strefabiznesu.pl/ladujesz-swojego-smartfona-w-ten-sposob-uwazaj-na-juice-jacking-wystarczy-chwila-zeby-cyberprzestepcy-zainfekowali-twoje/ar/c3-17791473 (dostęp 23.09.2023).

[11] Jako przykład wskazać można m. st. Warszawa, w którym udostępniane są publiczne porty USB m. in. na wielofunkcyjnych ekranach *Digital CityLight* (dostępność: Centrum 01, ul. Marszałkowska, Królikarnia 02, ul. Puławska, Zajezdnia Wola 03 i 06, Al. Solidarności, Muranów 03, ul. Anielewicza, Kapitulna 01, ul. Miodowa, Piękna 03 i Mokotowska 02, ul. Piękna, Wiejska 01, ul. Górnośląska – za: T. Szwast, *Przystanki, na których doładujesz telefon i sprawdzisz, gdzie jest autobus pojawiły się w Warszawie*, oiot.pl, 27.08.2021 (https://oiot.pl/digital-citylight-nowe-przystanki-w-warszawie/, dostęp 24.09.2023).

[12] https://www.gov.pl/web/mobywatel (dostęp 22.09.2023).

zakupem w salonie[13]. Wówczas nie tylko osoby, które same zainstalowały na swoich urządzeniach aplikacje rządowe, ale wszyscy użytkownicy mieliby na swoich urządzeniach dostęp do najwrażliwszych – i z punktu widzenia hakerów – najbardziej pożądanych danych wszystkich obywateli posiadających zarówno telefon jak i dowód tożsamości.

Mając powyższe na uwadze chciałbym – w trybie art. 13 ust. 1 pkt 2 ustawy z dnia 15 lipca 2023 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2023 r. poz. 1058) – prosić Pana Ministra o **informację o sposobie zabezpieczenia danych dostępnych w aplikacjach rządowych przed nieuprawnionym dostępem i przejęciem w sposób wskazany na wstępie, a mianowicie poprzez atak typu *juice jacking*.** Jakkolwiek pojawiają się w przestrzeni publicznej informacje obejmujące sposób przeciwdziałania cyberatakom w tejże przestrzeni[14], a także złośliwemu oprogramowaniu, to jednak będę wdzięczny za szersze odniesienie się do zasygnalizowanego przeze mnie w niniejszym wystąpieniu problemu.

Niezależnie od powyższego deklaruję także możliwość zaangażowania się ekspertów Biura Rzecznika Praw Obywatelskich w ewentualne dalsze prace analityczne dedykowane temu zagadnieniu.

Łączę wyrazy szacunku,

---

[13] M. Fraser, *Rządowe aplikacje na smartfonach. Najważniejsze pytania bez odpowiedzi*, CyberDefence24, 30.11.2022 (https://cyberdefence24.pl/polityka-i-prawo/rzadowe-aplikacje-na-smartfonach-najwazniejsze-pytania-bez-odpowiedzi, dostęp 24.09.2023). Zgodnie z art. 64 projektu ustawy o ochronie ludności oraz o stanie klęski żywiołowej „*autoryzowany sprzedawca, o ile jest to techniczne możliwe, obowiązany jest do preinstalacji aplikacji mobilnej RSO na telekomunikacyjnych urządzeniach końcowych sprzedawanych użytkownikom*" (wersja z dnia 31 sierpnia 2022 roku, ostatnia aktualizacja na stronie 18 listopada 2022 roku – projekt dostępny na stronie https://legislacja.rcl.gov.pl/projekt/12363754/katalog/12909380#12909380, dostęp 27.09.2023). W wersji projektu rozpatrywanej przez Komisję Prawniczą (stan na dzień 31 maja 2023 roku) w ustawie z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (Dz. U. z 2023 r. poz. 748) w art. 20a po ust. 1 dodaje się ust. 1a w brzmieniu: „1a. *Dostawca usług telekomunikacyjnych ruchomej publicznej sieci telekomunikacyjnej w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz.U. z 2022 r. poz. 1648, 1933 i 2581), o ile jest to technicznie możliwe, obowiązany jest do preinstalacji aplikacji mobilnej Alarm112 na telekomunikacyjnych urządzeniach końcowych sprzedawanych użytkownikom w autoryzowanych punktach sprzedaży*.", etap Komisji Prawniczej dostępny na stronie https://legislacja.rcl.gov.pl/projekt/12363754/katalog/12909416#12909416 (dostęp 27.09.2023).

[14] Między innymi: „*Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych*", 2014 (https://cyberprofilaktyka.pl/pliki/4-zagrozenia_cyberprzestrzeni_produkt_finalny.pdf, dostęp 25.09.2023); „*Cyberzagrożenia w systemie finansowym 2022*" (https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf, dostęp 25.09.2023).

Marcin Wiącek

Rzecznik Praw Obywatelskich

/-podpisano elektronicznie/