Gmina Mielec
ul. Głowackiego 5, 39-300 Mielec
Godziny pracy Urzędu: pon.: 7:30 - 17:00, Wt. - Czw.: 7:30 - 15:30, Pt.: 7:30 - 14:00
Telefon: 17 773 05 90 Fax: 17 773 05 91 Email: sekretariat@ug.mielec.pl

Poradnik CERT Polska o zagrożeniach związanych z klikaniem w podejrzane linki

2023-03-16 11:33:16

Pełna treść ostrzeżenia dostępna w komunikacie "Nie klikaj w podejrzane linki - czyli jak nie ostrzegać przed zagrożeniem" na stronie CERT.

W ostatnich latach temat cyberbezpieczeństwa zyskuje coraz większą popularność. Przy okazji pojawiają się różne rekomendacje związane z tym zagadnieniem. Na szczególną uwagę zasługują wszelkie zalecenia mówiące o „nieklikaniu w podejrzane linki", które zazwyczaj są tworzone w zestawieniu z alarmującymi tytułami, jak np.: „Kliknęła w link i straciła oszczędności". W tym artykule skupimy się na wytłumaczeniu dlaczego „kliknięcie w link" nie musi być niebezpieczne oraz przedstawimy argumenty za tym dlaczego porada przestrzegająca przed „podejrzanymi" linkami nie jest jasna i wymaga szerszego omówienia.

Sytuacja zazwyczaj wyglądała następująco: ktoś kliknął w link i trafił na stronę, która była łudząco podobna do strony internetowej banku lub portalu społecznościowego. Użytkownik nie dostrzegł różnicy i wpisał swoje dane do logowania. Oszuści wykorzystali wyłudzone dane, aby uzyskać dostęp do konta i środków ofiary. Z perspektywy użytkownika utrata środków mogła wyglądać na bezpośrednie następstwo kliknięcia w nieodpowiedni link. Jednak w rzeczywistości najistotniejszym problemem nie było samo kliknięcie w link, ale to, że strona, na której podał dane, była fałszywa. Należy podkreślić, że jest możliwe stworzenie strony o dowolnym wyglądzie. Dlatego też strony tworzone przez oszustów mogą wyglądać właściwie tak samo jak prawdziwe. W związku z tym należy zwracać szczególną uwagę na wszystkie formularze do podawania danych.

Zacznijmy od wyjaśnienia czym są linki

Linki (hiperłącza) to odnośniki, które umożliwiają użytkownikom internetu swobodne przemieszczanie się między materiałami i treściami na stronach internetowych lub między miejscami w danym dokumencie.

Wielu użytkownikom linki kojarzą się przede wszystkim z SMS-ami i wiadomościami email, gdzie najczęściej są widoczne jako klikalny adres strony zaczynający się zazwyczaj od http:// lub https://. Linki jednak mogą się także kryć pod dowolnym klikalnym elementem na stronie internetowej lub w wiadomości email.

Linki zawierają w sobie tekst widziany przez użytkownika oraz informację o docelowym adresie lub zasobie. Niektóre źródła radzą by skierować kursor myszki na link, co spowoduje wyświetlenie docelowego adresu URL w lewym dolnym rogu okna.

Należy jednak zwrócić uwagę, że dla przeciętnego użytkownika przeanalizowanie wyświetlonego linku lub adresu może okazać się trudne. Dodatkowo, ten sposób nie sprawdzi się w przypadku powszechnie stosowanych dziś skracaczy, czyli narzędzi, które pozwalają zamienić długi adres internetowy na zaledwie kilka znaków. Jeśli takie narzędzie zostało zastosowane, to poznanie domeny docelowej będzie możliwe dopiero po wejściu we wskazany link.

Czy kliknięcie w link może być niebezpieczne?

Warto to podkreślić, samo kliknięcie w link w znaczącej większości przypadków nie jest niebezpieczne. Dopiero akcje wykonane na stronie lub zawartości kontrolowanej przez oszustów mogą przynieść szkody.

Jednak od każdej reguły musi istnieć wyjątek i o nim też musimy powiedzieć. Są to podatności, czyli błędy i luki w oprogramowaniu. Przestępcy mogą je wykorzystać, aby poprzez stronę internetową uzyskać dostęp do jakichś zasobów, które normalnie powinny być niedostępne bez dodatkowej interakcji ze strony użytkownika. Jednak nie powinniśmy się tego obawiać jeżeli na bieżąco aktualizujemy oprogramowanie - zabezpiecza to nas przed ich wykorzystaniem.

Oczywiście możliwe jest, że staniemy się ofiarą ataku wykorzystującego nieznane podatności, jednak jest to niezwykle mało prawdopodobne. Wynika to z faktu, że znalezienie takowych w dojrzałym oprogramowaniu jest trudne, więc koszt takiego ataku jest bardzo wysoki. Warto też wspomnieć, że nie są znane masowe kampanie, w których atakujący na dużą skalę wykorzystywaliby nieznane podatności - spowodowałoby to ich natychmiastowe wykrycie przez specjalistów.

Kiedy linki możemy uznać za podejrzane?

Na ogół nasze wątpliwości budzą te wiadomości, których się nie spodziewamy. Jednak oszuści, aby uśpić naszą czujność, wysyłają wiadomości nie wzbudzające podejrzeń, czyli takie, które faktycznie moglibyśmy otrzymać. Należy bowiem pamiętać, że wiadomości phishingowe są bardzo często podobne do prawdziwych komunikatów różnych usługodawców. Dla przeciętnego odbiorcy, który nie dysponuje wiedzą o technikach stosowanych przez oszustów, weryfikacja nadawcy może się okazać utrudniona.

Należy podkreślić, że możliwe jest sfałszowanie pola nadawcy w wiadomości SMS. Przestępcy mogą zrobić to za pomocą ogólnodostępnych narzędzi. Analogiczna sytuacja ma miejsce w przypadku wiadomości mailowych. Chociaż nazwa nadawcy może wskazywać na jakąś firmę lub się z nią kojarzyć, to w rzeczywistości nie powinniśmy brać tego jako wyznacznik prawdziwości wiadomości. Możliwa jest bowiem sytuacja, że dana wiadomość została wysłana przez kogoś innego.

Warto też pamiętać, że linki do stron o charakterze phishingowym są dystrybuowane nie tylko za pomocą wiadomości mailowych i SMSów. Można natknąć się na nie np. we wpisach na portalach społecznościowych i w prywatnych wiadomościach wysłanych z przejętych kont. Prowadzą one do stron podszywających się pod zadany podmiot i ich celem jest zachęcenie do podania poufnych informacji.

Nadal popularne są też oszustwa na platformach aukcyjnych, gdzie sprzedawcy otrzymują linki do stron, na których rzekomo można odebrać pieniądze za sprzedany przedmiot. Na stronach tych użytkownik proszony jest o podanie danych karty płatniczej lub wyświetlana mu jest spreparowana strona logowania swojego banku.

Ostatnio linki do stron phishingowych są zamieszczane także w reklamach w wyszukiwarce i wyglądają jak zwykłe wyniki wyszukiwania.

Jak więc możemy się uchronić przed podaniem danych na fałszywej stronie?

Za każdym razem, gdy widzimy stronę, która prosi nas o dane, a w szczególności, gdy zobaczymy jakiś panel logowania, należy dokładnie sprawdzić na jakiej stronie rzeczywiście się znaleźliśmy.

Możemy to zrobić jedynie poprzez sprawdzenie domeny strony, na której jesteśmy (np. teraz jesteście na domenie cert.pl). Nazwa domeny znajduje się w pasku adresu i jest zazwyczaj oznaczona nieco innym kolorem. Należy ją porównać z domeną, którą zawsze widzimy, gdy się logujemy do danego serwisu.

Warto rozważyć też użycie menedżera haseł. Menadżer haseł nie tylko ułatwi nam korzystanie z internetu, bo nie będziemy musieli pamiętać wszystkich haseł do kilkunastu lub kilkudziesięciu różnych usług internetowych, z których korzystamy, ale przede wszystkim zwiększy nasze bezpieczeństwo. Jeśli menadżer haseł oferuje integrację z przeglądarką np. w formie wtyczki lub jest już w nią wbudowany, to taki menadżer haseł powiąże hasło z daną stroną i pozwoli na jego uzupełnienie tylko na prawdziwej stronie.

Innym dobrym sposobem jest korzystanie z kluczy bezpieczeństwa FIDO2. Są to wygodne i łatwe w użyciu urządzenia, które wystarczy nosić ze sobą i

wpiąć w port USB komputera albo przyłożyć do telefonu, gdy chcemy się zalogować.

Dodatkowo, w przypadku operacji bankowych przed potwierdzeniem ich, należy dokładnie przeczytać opis w SMS-ie z kodem lub powiadomieniu w aplikacji bankowej i sprawdzić czy rodzaj operacji oraz kwota się zgadzają.

Dziękujemy za odwiedziny i zapraszamy ponownie

bezpośredni link do strony www