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

Ostrzeżenie CERT Polska o kampanii phishingowej na serwisy pocztowe

2023-04-04 14:58:18

Pełna treść ostrzeżenia dostępna w komunikacie "Kampanie phishingowe na serwisy pocztowe" na stronie CERT.

- **Szczególnie narażeni użytkownicy: Wszyscy internauci**
- **Wektor ataku: Wiadomości e-mail**
- **Możliwe skutki: Przejęcie konta przez przestępców**
- **Atakowane platformy: Różne**

Jednym z najczęstszych zagrożeń dla internautów, obserwowanych przez nasz zespół, pozostaje phishing. Pozornie nieszkodliwe maile, często wzywające do pilnego działania, mogą prowadzić do fałszywych witryn wyłudzających dane.

Schemat działania

Głównym celem sprawców tego oszustwa jest wyłudzenie poufnych informacji (najczęściej danych dostępowych do konkretnej usługi) poprzez podszycie się pod dany podmiot lub osobę. W tym celu przestępcy rozsyłają do potencjalnych ofiar wiadomości mailowe zawierające link do kontrolowanej przez siebie witryny. Należy przy tym podkreślić, że nie ma jednego schematu szkodliwych wiadomości stosowanego przez oszustów - różnice wynikają z wytypowanej grupy będącej celem ataku oraz możliwości technicznych sprawców. Często powtarzający się element to wywieranie presji czasu na odbiorcy poprzez wzywanie go do podjęcia natychmiastowych działań i zwracanie uwagi na nieodwołane, uciążliwe konsekwencje ich zaniechania. Gdy ofiara otworzy link i zaloguje się na podstawionej przez oszustów stronie, wówczas jej dane uwierzytelniające trafią w ręce przestępców, którzy uzyskają w ten sposób dostęp do jej konta. Kolejnym krokiem jest na ogół zmiana hasła dostępowego, co skutkuje odcięciem prawowitego właściciela od konta.

Najczęstszym i najmniej wyrafinowanym schematem, który jest często odnotowywany przez nasz zespół, jest po prostu masowa wysyłka wiadomości phishingowych pod przypadkowe adresy mailowe. Nadawcy bardzo często podszywają się w takich wiadomościach pod administratorów poczty elektronicznej (w nazwie nadawcy) i informują np. o blokadzie konta z tytułu wykrytego naruszenia. Maile tego typu są często napisane bardzo słabą polszczyzną i usiłują imitować oficjalne, automatycznie wygenerowane powiadomienie. Umieszczony w wiadomości link prowadzi do strony internetowej, która prezentuje prosty formularz logowania, niekiedy zawierający wyłącznie pola do podania nazwy użytkownika i hasła (które często nie jest nawet maskowane tzn. widać wprowadzone w nim znaki).

Czasami kampanie tego typu są ukierunkowane na użytkowników konkretnego dostawcy usług. Wówczas fałszywa strona logowania może próbować wzbudzić zaufanie np. poprzez zamieszczony logotyp.

Trzeba jednak pamiętać, że często przestępcy zamiast masowej wysyłki słabo przygotowanych wiadomości phishingowych przygotowują ukierunkowane ataki na użytkowników konkretnych dostawców. Rozsyłane wówczas wiadomości bazują na tych samych schematach - podszywanie się pod administrację i tworzenie presji czasu pod groźbą negatywnych konsekwencji - jednak są już dużo lepiej przygotowane.

Takie wiadomości prowadzą nierzadko do stron, które wizualnie bardzo dobrze imitują prawdziwy panel logowania. Wskazówkę, że może to być phishing stanowią niedziałające elementy interfejsu (takie jak linki „zapomniałem hasła" czy pola „nie wylogowuj mnie").

Zdarza się, że fałszywe witryny bardzo pieczołowicie odtwarzają rzeczywiste serwisy. Mogą zawierać wszystkie elementy prawdziwej witryny, w tym reklamy oraz powiadomienie o wykorzystywaniu ciasteczek (cookies). Z tego powodu bardzo istotne jest uważne sprawdzanie, czy domena w pasku adresowym zgadza się z rzeczywistym adresem serwisu.

Wiadomości phishingowe mogą być też bardziej zakamuflowane i wyłamywać się z opisanych powyżej schematów. Wówczas treść wiadomości nie odnosi się w żaden sposób do skrzynki pocztowej, lecz odsyła do jakiegoś zasobu, do którego rzekomo prowadzi umieszczony w niej link. Nadawcy mogą w nich podszywać się pod różne firmy lub instytucje, wykorzystując autentyczną stopkę i informować np. o nowej fakturze czy innym dokumencie.

Po kliknięciu w link znajdujący się w wiadomości użytkownik przenoszony jest na witrynę zawierającą prosty panel logowania lub podszywającą się pod konkretnego dostawcę usług. Bardzo często potencjalna ofiara jest informowana, że w celu uzyskania dostępu do danego zasobu konieczna jest autoryzacja (poprzez podanie danych logowania).

Ważne informacje

Twórcy przeglądarek internetowych wkładają wiele wysiłku w izolowanie potencjalnie złośliwych stron internetowych od systemu operacyjnego - w praktyce nie obserwujemy przypadków, by samo wejście na stronę phishingową niosło za sobą negatywne konsekwencje. Dopiero po wprowadzeniu danych do formularza trafiają one w ręce przestępców.

Jak się chronić?

W celu ochrony przed phishingiem warto rozważyć skorzystanie z menadżera haseł i skonfigurować go w taki sposób, aby automatycznie uzupełniał formularz logowania. Wówczas rozróżnienie prawdziwej witryny od fałszywej przejmuje automat, który w tym drugim przypadku nie wypełni formularza logowania.

W przypadku otrzymania wiadomości mailowej należy zwracać szczególną uwagę, czy adres nadawcy nie budzi wątpliwości. Ponadto warto uważnie czytać treść maila - wiadomości oszustów, choć często po polsku, na ogół zawierają liczne błędy językowe i literówki. Przed logowaniem na dowolnej stronie należy sprawdzić, czy jej adres zgadza się z oczekiwaną domeną serwisu. W razie wątpliwości co do prawdziwości otrzymanej wiadomości lub strony internetowej zalecamy powstrzymanie się od podawania jakichkolwiek informacji i kontakt z pomocą techniczną danego dostawcy usług, lub przesłanie zgłoszenia do naszego zespołu za pośrednictwem formularza.

Również włączenie dwuskładnikowego uwierzytelnienia (2FA) może stanowić dodatkową warstwę ochrony przed phishingiem, jednak jest ona skuteczna jedynie przeciwko najbardziej prymitywnym stronom phishingowym, które po prostu nie wyłudzają od użytkownika drugiego składnika. Stosowanie unikalnych, nieschematycznych haseł do poszczególnych serwisów pozwoli natomiast ograniczyć szkody w przypadku, gdy oszustom jednak uda się wyłudzić hasło.

Co zrobić w przypadku, gdy doszło do wyłudzenia danych

Należy jak najszybciej skontaktować się z administratorem danej usługi i poinformować o zaistniałej sytuacji. CERT Polska nie ma możliwości udzielenia pomocy w odzyskaniu przejętego konta, jednak zachęcamy do przesłania zgłoszenia do naszego zespołu za pośrednictwem formularza na stronie Zgłoś incydent CERT.PL i przekazanie adresu szkodliwej witryny - umożliwi nam to podjęcie działań w celu zablokowania zagrożenia i ochrony pozostałych internautów.

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

Dziękujemy za odwiedziny i zapraszamy ponownie

bezpośredni link do strony www