https://policja.pl/pol/aktualnosci/212455,Top-5-najczestszych-technik-phishingowych.html
2022-01-19, 14:42

TOP 5 NAJCZĘSTSZYCH TECHNIK PHISHINGOWYCH

Data publikacji 30.12.2021

Phishing to rodzaj oszustwa, który polega na podawaniu się za inną osobę, podszywaniu się pod firmę lub instytucję w celu wyłudzenia poufnych informacji, danych logowania, danych karty kredytowej, konta bankowego lub używanych haseł. Liczba oszustw tego rodzaju nieprzerwanie rośnie od 2015 roku, najlepiej ukazują to statystki prowadzone przez zespół CERT Polska.

Fałszywa strona może być bardzo podobna do prawdziwej

Oszust może prowadzić ze sprzedawcą długą korespondencję. Będzie się starał zachowywać jak ktoś, kto rzeczywiście chce kupić towar.

Niektórzy orientują się w porę, niestety nie brakuje też osób okradzionych ze znacznych kwot.

Podanie pełnego numeru karty płatniczej oraz kodu CVC/CVV w fałszywym formularzu może spowodować wyprowadzenie wszystkich dostępnych środków z konta.

Ostatnie miesiące były rekordowe pod względem liczby zaobserwowanych prób oszustwa przez e-mail, SMS czy komunikator. Ten wzrost zbiega się z pandemią koronawirusa i związanym z nią ograniczeniem kontaktów osobistych oraz przeniesieniem do internetu wielu codziennych aktywności. Większość ataków, z którymi możemy się zetknąć, stanowią proste sztuczki opierające się na powtarzalnych schematach i niewymagające dużych nakładów pracy. Ale jest ich wiele, więc przeciętny użytkownik naprawdę musi zachowywać czujność, by nie dać się złapać...

OSZUŚCI NA PLATFORMIE OLX

Najbardziej popularną kampanią phishingową, która pojawiła się w czasie pandemii COVID-19, jest oszustwo wobec użytkowników serwisu ogłoszeniowego OLX.

Chociaż scenariusz ataku z biegiem czasu jest modyfikowany, schemat, według którego działają atakujący, pozostaje niezmienny od niemal roku.

1. Przestępcy kontaktują się w sprawie zakupu przedmiotów wystawionych na sprzedaż, wykorzystując komunikator WhatsApp.

2. Proponują sfinalizowanie transakcji z wykorzystaniem usługi płatności, świadczoną przez portal. Jeśli sprzedawca się zgodzi, wysyłają spreparowany link, który swoją szatą graficzną, co prawda, przypomina OLX, ale zawiera fałszywy formularz płatności.

3. Na fałszywej stronie ofiara jest nakłaniana do podania szczegółowych danych karty płatniczej w celu rzekomego odebrania opłaty za wystawiony przedmiot (Uwaga! Serwis OLX świadczy usługę płatności, ale nigdy nie prosi o dane karty płatniczej ani dane logowania do konta bankowego).

4. Atak kończy się kradzieżą danych karty kredytowej i wyłudzeniem środków finansowych nieświadomego użytkownika.

FAŁSZYWE WIADOMOŚCI SMS

Kto z nas nie dostał nigdy SMS-a z informacją, że minął termin zapłaty jakiejś należności lub z innego rodzaju przypomnieniem? Takie wiadomości to wygodna i szybka forma komunikacji z zapominalskim klientem. Niestety przestępcy o tym wiedzą i tworzą fałszywe ponaglenia, celując w roztargnione osoby, które uwierzą, że rzeczywiście mają nieuregulowane rachunki.

Oszust wysyła swój SMS do jak największej liczby losowych numerów. W wiadomości umieszcza link do fałszywej strony płatności. Podobnie jak w przypadku omówionego wcześniej oszustwa, celem tego ataku jest wyłudzenie pieniędzy. Fałszywe SMS-y informują np. o konieczności dopłaty do szczepionki lub zachęcają do zarejestrowania się (odpłatnie) na szczepienie. Pojawiają się również wiadomości, których treść nie jest związana z pandemią, np. dotyczą uregulowania należności za energię elektryczną, wyrównania niedopłaty podatku lub mandatu karnego.

Kwota określona w wiadomości jest zwykle niewielka. Przestępcy liczą na to, że odbiorca nie będzie drobiazgowo weryfikował, czy należność jest zasadna. Czekają na osoby, które będą skłonne zapłacić „dla świętego spokoju". Niestety podanie danych logowania na fałszywej stronie płatności może doprowadzić do utraty dużo większej sumy niż wymieniona w wiadomości.

SZKODLIWE OPROGRAMOWANIE UKRYTE POD AKCEPTACJĄ REGULAMINU

Kampanie phishingowe mogą się rozprzestrzeniać również za pomocą wiadomości e-mail. Przykładem tego są fałszywe maile, które obserwujemy od prawie roku. Nadawcy podszywają się pod operatorów polskich serwisów pocztowych – Onet, Interia, O2 i Wirtualna Polska. Zależnie od wariantu oszustwa, w treści wiadomości pojawia się informacja o konieczności zatwierdzenia nowej polityki prywatności lub powiadomienie o tym, że konto zostało zablokowane z powodu naruszenia regulaminu przez użytkownika. W obu przypadkach ofiara jest namawiana do przejścia na wskazaną stronę w celu zdjęcia blokady konta. Jeśli otworzymy stronę w przeglądarce internetowej na komputerze, nasze urządzenie może zostać zainfekowane wirusem wykradającym poufne dane. Wejście na stronę przy użyciu telefonu z systemem Android wyświetla inną zawartość. Użytkownicy telefonów są nakłaniani do pobrania aplikacji, która ma rzekomo być wymagana do dokończenia procesu weryfikacji. Aplikacja ta w rzeczywistości jest szkodliwym

oprogramowaniem wykradającym dane bankowe.

URZĄDZENIA MOBILNE POD OSTRZAŁEM FLUBOTA

Pandemia koronawirusa spowodowała wzrost popularności zakupów online. To z kolei zachęciło atakujących do wykorzystania wizerunku firm kurierskich. Atak polega na zainstalowaniu na urządzeniu mobilnym szkodliwego oprogramowania Flubot. Swoją nazwę (z ang. flu – grypa) zawdzięcza błyskawicznemu rozprzestrzenianiu się. Atak jest skierowany w użytkowników urządzeń z systemem Android.

Fałszywa aplikacja uzyskuje dostęp do listy kontaktów z zainfekowanego urządzenia i uprawnienia, które pozwalają jej na wysyłanie i odbieranie SMS-ów. Dodatkowo Flubot jest zagrożeniem, które potrafi wykradać dane logowania do różnych serwisów, w tym bankowości mobilnej.

Smartfon jest trudniejszym celem dla przestępców niż laptop czy komputer stacjonarny. Systemy operacyjne nie pozwalają zainfekować urządzenia mobilnego złośliwym oprogramowaniem w sposób automatyczny – bez udziału użytkownika. Dlatego przestępcy starają się nakłonić nas, abyśmy sami zainstalowali wirusa, którego nam podrzucają. Ta sztuczka nie uda się w przypadku systemu iOS. Na urządzenia Apple'a w ogóle nie da się zainstalować aplikacji pochodzących spoza oficjalnego sklepu. Istnieje taka możliwość dla systemu Android, który jest otwarty dla oprogramowania z różnych źródeł. Podstawowym środkiem ostrożności powinno więc być instalowanie tylko aplikacji pobranych z oficjalnego sklepu Google Play.

FACEBOOK I FAŁSZYWE ARTYKUŁY

Stresujące, groźne, sensacyjne newsy łatwo się rozchodzą, zwłaszcza na portalach społecznościowych i w komunikatorach. Dlatego pandemia i termin COVID-19 są wykorzystywane do rozprowadzania wiadomości phishingowych. Niestety w takim przypadku link do „portalu informacyjnego" przychodzi od „znajomej osoby", więc łatwiej jest dać się nabrać. Oszuści działają przez cudze konta społecznościowe, do których hasło udało im się uzyskać w następujący sposób, czyli: wysyłają w komunikatorze lub publikują na profilu link do sensacyjnego newsa. Kto kliknie w ten link, zobaczy formularz logowania do Facebooka. Dawniej fałszywe wiadomości zawierały emocjonalny przekaz, np. informowały o rzekomym gwałcie na młodej osobie lub znęcaniu się nad zwierzętami. Przestępcy jednak bardzo łatwo modyfikują swoje plany działania, wykorzystali więc pandemię i zaczęli tworzyć artykuły ściśle związane z COVID-19. Fałszywe wiadomości dotyczące zgonu po szczepionce przeciw COVID lub informacje o śmierci spowodowanej koronawirusem mają zachęcać do wprowadzenia danych logowania w celu zapoznania się z treścią informacji.

To fałszywy formularz, więc jeśli podamy tam swoje dane logowania, to przestępca będzie mógł się zalogować na nasze konto i z niego wysyłać podobne wiadomości do naszych znajomych i w ten sposób przejmować ich konta. Po co komu tyle cudzych kont na Facebooku? Po to, żeby oszukać jak najwięcej osób i wzbogacić się ich kosztem.

Mając możliwość wysłania wiadomości do setek „znajomych", złodziej wysyła krótki komunikat, np.: Hej, masz może BLIK-a? Podasz mi kod? Potrzebuję pożyczyć 500 zł – oddam najpóźniej w przyszłym tygodniu.

Gdy dopytujemy, co się stało, rozmówca przedstawia sprawę jako pilną i kryzysową. Czasem chodzi o zepsuty samochód i opłatę za holowanie, czasem ktoś został okradziony w podróży przez kieszonkowców... Nieszczęścia chodzą po ludziach. Komuś znajomemu przecież pomożemy w trudnej sytuacji. Przestępcy liczą na to, że nie sprawdzimy, czy na koncie przyjaciela na pewno to właśnie on jest zalogowany. Kod BLIK można zrealizować wszędzie – np. w bankomacie na drugim końcu Polski. Wypłaconej gotówki ofiary nie odzyskują.

JAK SIĘ BRONIĆ?

Najlepszą linią obrony w przypadku kampanii phishingowych są zawsze ostrożność oraz uwaga. Za każdym razem należy weryfikować nazwę strony internetowej, na której podaje się wrażliwe dane, czy nazwę domeny, z której otrzymano ważną wiadomość mailową. Każdy błąd, nawet drobna literówka, mogą świadczyć o oszustwie. Bardzo istotne jest również używanie unikalnych i odpowiednio skomplikowanych haseł w każdym z serwisów (w szczególności podczas korzystania

z kont pocztowych, za pomocą których można resetować hasła w innych serwisach). Pomocne w tym zakresie są menedżery haseł. Wszelkie podejrzenia należy weryfikować, kontaktując się z rzekomym nadawcą za pomocą innego

kanału niż ten, przez który dotarła wiadomość.

Należy również pamiętać o odpowiednim dbaniu o inne kwestie związane z naszą obecnością w internecie. CERT Polska przygotował krótki poradnik dotyczący najważniejszych zasad bezpiecznego korzystania z poczty elektronicznej oraz mediów społecznościowych. Poradnik można znaleźć pod adresem: https://www.cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf.

Ponadto od marca 2020 r. CERT Polska wraz z operatorami telekomunikacyjnymi publikuje listę ostrzeżeń przed niebezpiecznymi adresami internetowymi. Zgodnie z założeniami na listę ostrzeżeń trafiają domeny internetowe, które za podstawowy cel swojego działania mają wprowadzenie w błąd użytkowników internetu. Operatorzy zobowiązali się m.in. do blokowania dostępu do stron internetowych, wykorzystujących nazwy domen internetowych opublikowanych na liście ostrzeżeń, a także do przekazywania do NASK-u informacji o takich stronach.

W 2020 r. aż 58 proc. domen znajdujących się na liście ostrzeżeń CERT Polska było powiązanych z fałszywymi panelami logowania do portalu Facebook. W tym roku CERT obserwuje ciągły wzrost szkodliwych domen wykorzystujących wizerunek platformy OLX – w 2020 r. zarejestrował 570 takich incydentów. Dla porównania – rok wcześniej było ich jedynie pięć.

W 2021 r. stanowią one prawie 30 proc. domen wpisanych na listę ostrzegającą przed niebezpiecznymi domenami.

Zachęcamy do przeczytania pozostałych artykułów z wydania specjalnego Gazety Policyjnej

CERT Polska

zdj. cert polska

film: st. sierż. Tomasz Lis

PLIKI DO POBRANIA

Deskrypcja do filmu
216.73 KB