Biuletyn Bezpieczeństwa Komputerowego

Ataki phishingowe

Ataki phishingowe stały się jednym z wiodących sposobów oszustów wykorzystywanych przez cyberprzestępców. Phishing to typ ataku, w którym przestępcy używając specjalnie spreparowanych wiadomości chcą wprowadzić ofiarę w błąd i nakłonić do wykonania czynności, której nie powinna wykonać, tak jak na przykład kliknięcie w szkodliwy link, podanie hasła czy otwarcie zainfekowanego załącznika. Atakujący nieustanie próbują udoskonalać sposoby swoich oszustw, tworząc coraz bardziej zaawansowane wiadomości phishingowe, które są lepiej spersonalizowane i trudniejsze do rozpoznania. Ataki phishingowe to nie tylko wiadomości e-mail. Oszuści korzystają również z takich technologii, jak wiadomości tekstowe SMS, media społecznościowe, a nawet połączenia telefoniczne. Oto ich najnowsze sposoby oszukiwania użytkowników oraz metody jak je rozpoznać.

Cyberprzestępcy zaczynają od rozpoznania

Wiadomości phishingowe były kiedyś łatwiejsze do wykrycia, ponieważ były to generyczne wiadomości wysyłane do wielu przypadkowych osób. Cyberprzestępcy nie mieli pojęcia, kto padnie ofiarą. Wiedzieli tylko, że im więcej wiadomości e-mail wyślą, tym więcej osób uda im się oszukać. Te prostsze ataki można było często wykryć szukając podejrzanych wiadomości e-mail z frazą "Drogi Kliencie", błędów ortograficznych lub wiadomości, które brzmiały zbyt piękne, aby mogły być prawdziwe, np. wiadomości o nigeryjskich dziedzicach tronów oferujących miliony dolarów.

W obecnych czasach cyberprzestępcy są o wiele bardziej wyrafinowani. Współcześnie atakujący prowadzą rozpoznanie swojej ofiary, tak aby stworzyć spersonalizowany atak. Zamiast rozsyłać wiadomości phishingowe do milionów osób lub podszywać się pod generyczne wiadomości wysyłane przez korporacje, mogą wysłać je do garstki osób i tak dostosować atak, aby wyglądał na wysłany przez kogoś, kogo znamy. Cyberprzestępcy szukają informacji:

- przeszukując profile w serwisie LinkedIn, informacje zamieszczane w mediach społecznościowych lub wykorzystując publicznie dostępne informacje lub znalezione w sieci TOR.
- wysyłając spreparowanie wiadomości, które wydają się pochodzić od kierownictwa, współpracowników lub sprzedawców, których znasz i z którymi pracujesz.
- dowiadując się jakie są zainteresowania użytkownika i wysyłając do niego wiadomość, podając się za kogoś, kto podziela wspólne zainteresowania.
- określając, że byłeś na konferencji lub właśnie wróciłeś z podróży, a następnie wysyłając wiadomości e-mail nawiązującej do podróży.

Cyberprzestępcy aktywnie wykorzystują inne metody dotarcia do ofiary, np. wysyłając te same wiadomości za pośrednictwem SMS-ów lub dzwoniąc bezpośrednio do niej.

W jaki sposób wykryć te bardziej zaawansowane ataki phishingowe

Przestępcy poświęcają dużo czasu na rozpoznanie swojej ofiary, dlatego wykrycie tego typu ataków może być trudne. Dobra wiadomość jest taka, że można je rozpoznać jeśli wiemy na co spojrzeć i czego szukać. Przed podjęciem jakichkolwiek działań z podejrzaną wiadomością należy zadać sobie następujące pytania:

1. Czy wiadomość wywołuje zwiększone poczucie pilności? Czy wywiera presję, aby ominąć zasady bezpieczeństwa obowiązujące w Twojej organizacji? Czy jesteś popędzany do popełnienia błędu? Im większa presja lub poczucie pilności, tym bardziej prawdopodobne, że jest to atak.
2. Czy wiadomość e-mail lub komunikat ma sens? Czy na pewno prezes firmy pilnie wysłałby do Ciebie SMS-a z prośbą o pomoc? Czy przełożony naprawdę wymaga, abyś w pośpiechu kupował karty podarunkowe? Dlaczego bank lub firma obsługująca karty kredytowe miałaby prosić o podanie danych osobowych, które powinna już posiadać? Jeśli wiadomość wydaje się dziwna lub masz jakiekolwiek obiekcje, może to oznaczać atak.
3. Czy otrzymujesz wiadomość e-mail związaną z pracą od współpracownika lub przełożonego, ale wiadomość ta została wysłana na prywatny adres e-mail?
4. Czy otrzymałeś e-mail lub wiadomość od kogoś, kogo znasz, ale sformułowanie, sposób pisma lub podpis w wiadomości są niewłaściwe lub nietypowe?

Jeśli wiadomość wydaje się dziwna lub podejrzana, może to być atak. Jedną z możliwości sprawdzenia czy otrzymana wiadomość jest prawdziwa, jest zadzwonienie pod znany ci numer kontaktowy osoby lub organizacji wysyłającej wiadomość.

Pamiętaj, że to Ty jesteś dla siebie najlepszą ochroną. Zdrowy rozsądek to podstawowa linia obrony.

Redaktor gościnny

Phil Hoffman jest emerytowanym konsultantem IT z 40-letnim doświadczeniem, koncentrującym się na infrastrukturze i bezpieczeństwie. Jest wieloletnim współpracownikiem i redaktorem biuletynu komputerowego OUCH!, a jego pasją jest technologia, jazda na rowerze i fotografia.

Źródła

Ataki socjotechniczne: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Najpopularniejsze oszustwa w mediach społecznościowych: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Wykryj i zatrzymaj ataki w wiadomościach tekstowych: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Ataki i oszustwa telefoniczne: https://www.sans.org/newsletters/ouch/vishing/
Odszukaj siebie w sieci: https://www.sans.org/newsletters/ouch/search-yourself-online/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz