SOPHOS

Security made simple.

Komentarz Mariusza Rzepki,
Senior Manager Eastern Europe w Sophos

- Na każde 39 sekund w sieci przypada jedna próba ataku hakerskiego[1].
- W samym pierwszym półroczu ubiegłego roku ponad połowa wszystkich wykradzionych danych pochodziła z mediów społecznościowych – to 56,18 procent[2].
- W ciągu ostatnich 5 lat na całym świecie hackerzy przejęli niemal 1,3 miliardów kont w mediach społecznościowych[3].
- Eksperci Sophos informują o nowych metodach hackerów, którzy próbują przejąć konta na Instagramie.

Naruszasz czyjeś prawa autorskie na Instagramie? Sprawdź, czy aby na pewno

W maju tego roku polski Instagram miał już prawie 6,5 miliona użytkowników[4] – ponad jedna trzecia z nich plasuje się w przedziale wiekowym od 18 do 24 lat. Przeglądamy codziennie zdjęcia w bajkowych sceneriach i udostępniamy relacje z naszego życia, nie zastanawiając się zbytnio nad informacjami, którymi się dzielimy. Co jednak, gdy dostaniemy wiadomość z sugestią, że naruszamy czyjeś prawa autorskie? Pierwszą reakcją będzie kliknięcie w link podany w e-mailu… Na to właśnie liczą hackerzy.

Na każde 39 sekund w sieci przypada jedna próba ataku hakerskiego[5]. Jedna sekunda wystarczy, aby uzyskano nieuprawniony dostęp aż do 69 rekordów: loginów, emaili czy haseł. W samym pierwszym półroczu ubiegłego roku ponad połowa wszystkich wykradzionych danych pochodziła z mediów społecznościowych – to 56,18 procent[6].

To na pierwszy rzut oka brzmi dziwnie. Dlaczego ktoś chciałby włamać się na konto na Instagramie, zamiast spróbować uzyskać dostęp do konta bankowego, hasła RDP czy portfela z kryptowalutami? Z drugiej strony, media społecznościowe to szczególne miejsce, w którym jesteśmy skłonni do dzielenia się bardzo prywatnymi informacjami. Niektórzy swobodnie wysyłają znajomym takie dane jak numer dowodu, potrzebny np. przy rezerwacji lotu lub noclegu, ale z naszymi bliskimi czy współpracownikami rozmawiamy również o sprawach służbowych, statusie majątkowym czy życiu prywatnym.

W ten sposób osoba dysponująca dostępem do naszego konta może dowiedzieć się o nas znacznie więcej niż gdyby włamała się do konta bankowego czy skrzynki e-mail. Co więcej, może wykorzystać profil do bezpośredniego kontaktu z naszymi znajomymi – wystarczy przywołać przykład „oszustw na BLIK-a". Zagrożenie jest realne: w ciągu ostatnich 5 lat na całym świecie hackerzy przejęli niemal 1,3 miliardów kont w mediach społecznościowych[7]. W tym celu wykorzystują różnorodne metody.

---

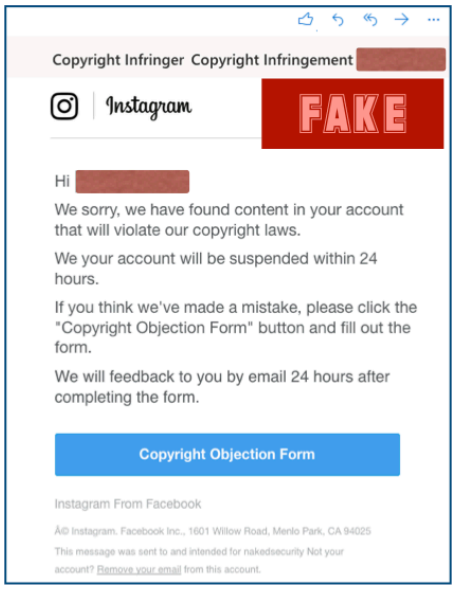
[1] University of Maryland
[2] Breach Level Index
[3] Bromium
[4] Statista
[5] University of Maryland
[6] Breach Level Index
[7] Bromium

SOPHOS

Security made simple.

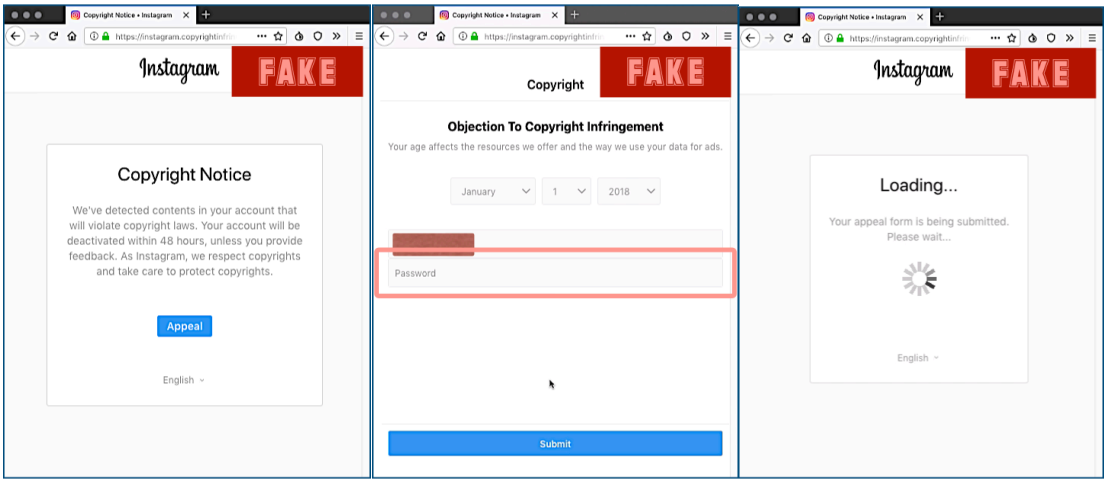
W ubiegłym miesiącu eksperci Sophos donosili o e-mailach informujących o udaremnieniu rzekomej próby zalogowania do konta na Instagramie i zachęcających do wpisania kodu uwierzytelniającego, aby potwierdzić swoją tożsamość – rzecz jasna, na fałszywej witrynie łudząco przypominającej popularny portal. Tym razem oszuści wykorzystują obawy użytkowników przed zablokowaniem profilu.

E-maile rzekomo wysłane przez portal społecznościowy informują, że materiały udostępnione przez użytkownika naruszają prawa autorskie, a konto zostanie zablokowane w ciągu 24 godzin. Jednocześnie wiadomość zachęca do podjęcia polemiki z tą decyzją.



Media społecznościowe to dla wielu osób stały element życia – każdego dnia internauci korzystają z nich przez średnio 2,5 godziny[8]. To nie tylko komentowanie postów na Facebooku czy Instagramie, ale również wymiana wiadomości z rodziną, znajomymi czy współpracownikami. Zablokowanie konta wiąże się przede wszystkim z utrudnionym kontaktem z naszym otoczeniem.

Nic więc dziwnego, że pokusa kliknięcia w odnośnik podany w e-mailu jest spora. Jeśli publikujemy tylko swoje zdjęcia i doskonale wiemy, że nie naruszyliśmy niczyich praw autorskich, sprawa nie może być trudna. Wypełnienie formularza to łatwa procedura – wyrażamy chęć odwołania się od decyzji, wpisujemy naszą datę urodzenia, login oraz hasło do konta…



Następnie zobaczymy stronę ładowania, po której zostaniemy poinformowani, że odwołanie zostało pomyślnie wysłane – i zostaniemy przekierowani na prawdziwą stronę portalu. Wtedy jednak może już być za późno na próbę zalogowania się…

[8] GWI

SOPHOS

Security made simple.

Co charakteryzuje ten atak? Dlaczego ma szansę powodzenia?

- **Jest skierowany na urządzenia mobilne**. Mimo wszystkich ich zalet, mają one zdecydowanie mniejszy ekran, co oznacza, że zwracamy mniejszą uwagę na szczegóły. Mobilne przeglądarki czy aplikacje nie ułatwiają sprawy – często ograniczają dostęp do tak prostych funkcji jak sprawdzenie certyfikatu strony czy pełnego nagłówka wiadomości e-mail. Dodajmy do tego fakt, że wielu użytkowników korzysta z smartfonów czy tabletów w biegu, podczas spotkań lub wracając po ciężkim dniu pracy do domu.
- W takich okolicznościach łatwo się rozproszyć i nie zwrócić uwagi na **literówki czy błędy gramatyczne**, których w fałszywej wiadomości nie brakuje. Mało kto również pomyśli o podejrzeniu pełnego adresu strony – na małym ekranie zobaczymy tylko nagłówek „instagram.copyright…". Dopiero po rozwinięciu zobaczymy, że adres kończy się domeną .cf, przypisaną Republice Środkowoafrykańskiej.
- **Zastosowanie elementów graficznych znanych z Instagrama** w wiadomości oraz na fałszywej stronie to standard w phishingu. Jednak warto zwrócić uwagę na nadawcę e-maila – wiadomość została wysłana z tureckiej firmy hostingowej. Profesjonalne poradniki dla użytkowników czy szkolenia dla pracowników z wykorzystaniem oprogramowania takiego jak Sophos Phish Threat, uczą zwracania uwagi na takie smaczki.
- Hackerzy zakładają, że **atakowany użytkownik nie zna procedur** stosowanych przez serwisy, które imitują. W przypadku otrzymania wiadomości od portalu społecznościowego, warto zalogować się na swoje konto samodzielnie – nie przez odnośnik w e-mailu. Pomaga również wykorzystanie menedżerów haseł, które nie będą automatycznie wpisywać danych do logowania na fałszywej stronie.

Kontakt dla mediów:
Karolina Sobieszek
Karolina.sobieszek@cluepr.pl