aut. Szymon Palczewski 20.11.2020

PROMOCJA NA BLACK FRIDAY? CHIŃSCY CYBERPRZESTĘPCY ROZKRĘCAJĄ HANDEL DANYMI

Chińscy cyberprzestępcy wykradają dane kart płatniczych klientów wirtualnych sklepów, tworząc fikcyjne witryny e-commerce. Aby zwiększyć skuteczność kampanii zakładają strony promujące spreparowane strony w social mediach oraz korzystają z reklam online, co jest szczególnie widoczne przed zbliżającym się Black Friday. W ten sposób czerpią zysk z dwóch źródeł: sprzedaży wadliwych towarów oraz handlu skradzionymi danymi na czarnym rynku.

Od początku pandemii COVID-19 coraz więcej osób korzysta z cyfrowych rozwiązań w czasie codziennych czynności, w tym zakupów online. Cyberprzestępcy starają się to sprawnie wykorzystać generując zysk. Obszarem szczególnie podatnym na wrogie działania jest handel elektroniczny, który daje możliwość przeprowadzenia prostych kampanii przynoszących zarobek.

Problem staje się jeszcze większy w okresie tuż przed i w trakcie Black Friday (27 listopada br.), kiedy konsumenci są kuszeni do zakupów online za pomocą wysokich rabatów. „Święto promocji" jest idealnym momentem dla cyberprzestępców, którzy „żerują" na osłabionej czujności użytkowników, pochłoniętych „szałem zakupów" – wskazują specjaliści Gemini Advisory w raporcie „Chinese Scam Shops Lure Black Friday Shoppers".

> *W ostatnich miesiącach od wybuchu pandemii banki w Europie oraz Stanach Zjednoczonych doświadczyły gwałtownego wzrostu liczby oszustw w handlu elektronicznym powiązanych z Chinami*
>
> *Raport „Chinese Scam Shops Lure Black Friday Shoppers"*

Według danych przedstawionych w raporcie, 200 z 600 złośliwych witryn e-commerce było połączonych z chińskim bankiem Jilin Jiutai Rural Commercial Bank Co. Strony te nie zostały zainfekowane złośliwym oprogramowaniem poprzez cyberataki, lecz powstały jako witryny przeznaczone do oszustw internetowych. Witryny wykradały dane kart płatniczych od nieświadomych kupujących, a następnie cyberprzestępcy sprzedali je na innych platformach w darknecie.

„Atrakcyjny" sklep? Tak, to pułapka

Podczas prowadzenia badań specjaliści Gemini Advisory zidentyfikowali grupę cyberprzestępców z Państwa Środka, która specjalizowała się w oszustwach w handlu elektronicznym. To ona odpowiada za znaczny wzrost incydentów w ostatnim czasie, obsługując setki witryn. W raporcie podkreślono, że ekspertom udało się ujawnić dziesiątki tysięcy rejestrów kart płatniczych ze Stanów Zjednoczonych

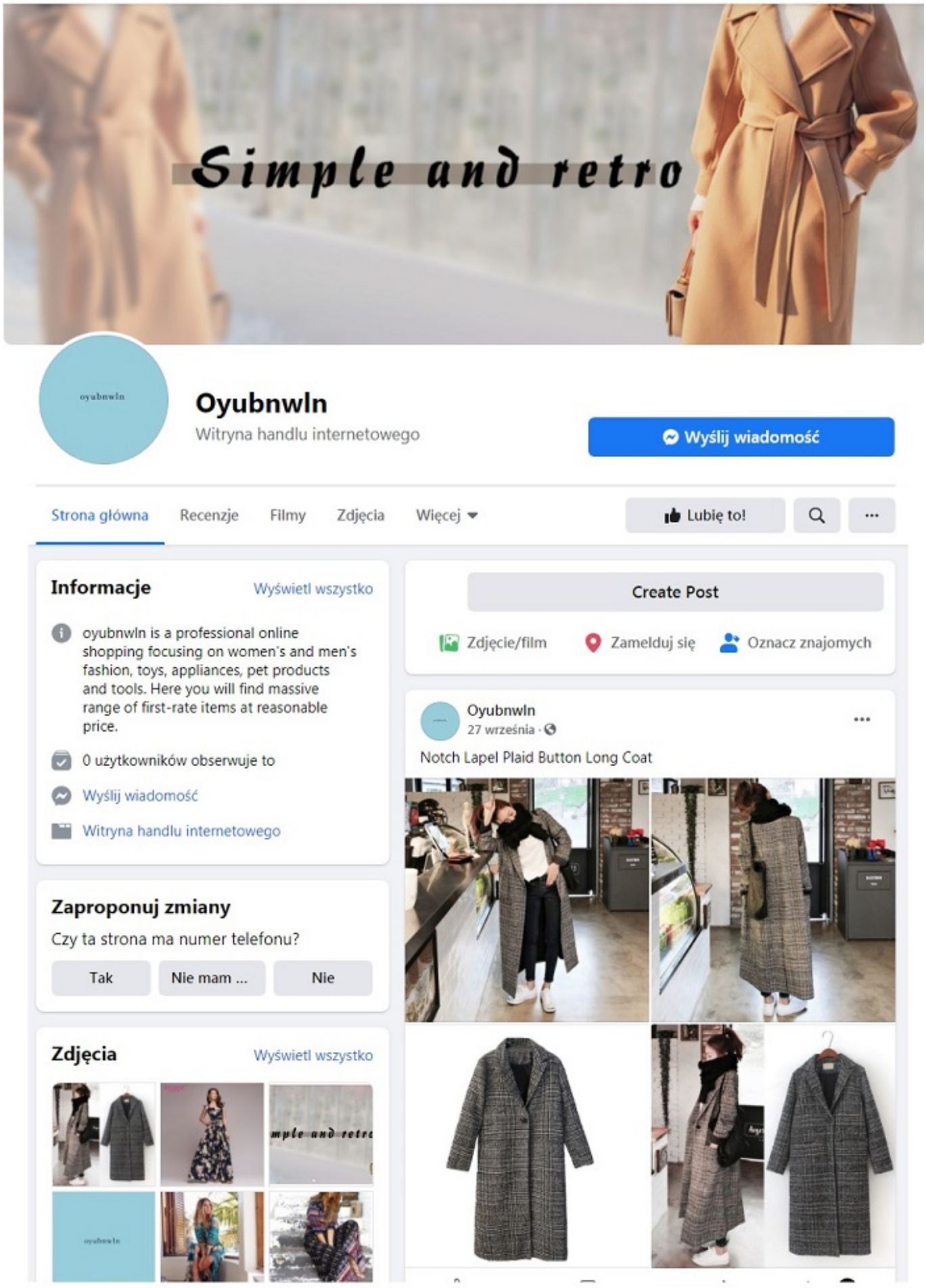
oraz innych państw, a także dane osobowe ofiar z sześciu ostatnich miesięcy.

Mechanizm działania chińskich cyberprzestępców nie jest skomplikowany. Najpierw tworzą sklep internetowy, aby reklamować i sprzedawać swoje towary. W rzeczywistości witryny służą do wykradania danych kart płatniczych klientów, które następnie są sprzedawane w darknecie.

Tego typu kampanie pozwalają cyberprzestępcom osiągnąć podwójny zysk. Po pierwsze, korzyści finansowe płynące ze sprzedaży podrobionych, wadliwych lub nieistniejących produktów. Po drugie, dochód z obrotu skradzionymi danymi.

> *Chińska grupa osiągnęła zyski w wysokości 500 000 USD w ciągu ostatnich sześciu miesięcy tylko ze sprzedaży skradzionych danych kart płatniczych w darknecie. Jednak łączne zyski przestępców są prawdopodobnie znacznie większe w oparciu o nielegalną sprzedaż wadliwych, podrobionych lub nieistniejących towarów*
>
> *Specjaliści Gemini Advisory*

Podczas kampanii cyberprzestępcy stworzyli setki witryn przeznaczonych do oszustw, a po ich uruchomieniu pracowali nad zwiększeniem ich widoczności oraz zasięgu, wykorzystując między innymi media społecznościowe, w tym Facebooka. W celu zwiększenia wiarygodności oraz popularności „sklepów" powstawały fanpage. Co warte podkreślenia, specjaliści Gemini Advisory zaobserwowali opóźnienie między uruchomieniem witryn a utworzeniem stron na social mediach, co sugeruje, że jest to nowa taktyka stosowana przez chińskich cyberprzestępców.



Fot. Fanpage przykładowego sklepu zarządzanego przez chińskich cyberprzestępców / Facebook

Jak tłumaczą eksperci, z punktu widzenia przeciętnego użytkownika nie widać żadnego połączenia czy korelacji między różnymi stworzonymi przez cyberprzestępców witrynami. Każda z nich wydaje się być odrębnym, legalnym sklepem.

Ponadto, strony te wykorzystują na przykład Google Ads oraz kampanie reklamowe w mediach społecznościowych, aby przyciągać klientów ofertami produktów ze zniżką poniżej ofert rynkowych. Promocje prawie zawsze wskazują, że oferty są częścią ograniczonej czasowo sprzedaży, która ma na celu zmuszenie potencjalnych klientów do dokonania zakupu. W raporcie przedstawiono przykład reklamy, gdzie podkreślono, że firma wycofuje się z rynku ze względu na kryzys związany z COVID-19 i promocja jest efektem wyprzedaży asortymentu, aby zminimalizować straty oraz pozbyć się zalegających produktów.

Wybuch pandemii koronawirusa spowodował, że coraz więcej osób decyduje się na korzystanie z wirtualnych rozwiązań bardziej niż dotychczas. Jednym z tego typu obszarów są zakupy online, zwłaszcza w czasie Black Friday, kiedy to mają miejsce wysokie rabaty i promocje, zachęcające konsumentów do „masowego” nabywania towarów. Atrakcyjne ceny zmniejszają czujność klientów, co sprawnie wykorzystują cyberprzestępcy. Kluczem do bezpieczeństwa niezmiennie pozostaje rozsądek i uwaga.

Czytaj też: Uwaga wyłudzenie! Atak na konto bankowe w 3 krokach