**Black Friday czasem łowów nie tylko dla kupujących.**

**Black Friday oraz Black Week to czas wyjątkowych okazji zakupowych, a jednocześnie wzmożonej aktywności cyberprzestępców. Analitycy Check Point Research ostrzegają, że w tym okresie zauważyli niemal dwukrotny wzrost witryn internetowych i wiadomości phishingowych związanych z Black Friday!**

W tygodniach poprzedzających Black Friday i Cyber Monday liczba nowo zarejestrowanych stron internetowych wzrosła w 2024 roku aż o 89% w porównaniu do 2023 roku, a w stosunku do 2022 roku – ponad trzykrotnie. Większość tych witryn to tzw. strony „zaparkowane”, pełne reklam i linków. Niemniej, około 3% z nich jest uznawanych za złośliwe, co czyni je potencjalnym zagrożeniem.

**Strony zaparkowane (ang. parked)** - domeny, które zostały zarejestrowane, ale nie są aktywnie używane do prowadzenia pełnoprawnej witryny internetowej. Zamiast tego wyświetlają one podstawowy lub tymczasowy content (np. reklamy, rankingi), często generowany automatycznie

Większość ze złośliwych stron podszywa się pod znane marki (m.in. Rolex, Louis Vuitton, J.Crew), ale także atakuje klientów mniejszych. Często wyglądają one bardzo podobnie do oryginalnych witryn, co – zdaniem ekspertów - sugeruje skoordynowaną działalność cyberprzestępców. Oto adresy przykładowych fałszywych witryn:

l **Stüssy (amerykańska marka odzieżowa)**: stussycanadablackfriday[.]com

l **Longchamp (francuska marka modowa, specjalizująca się w torebkach)**: longchampblackfriday[.]com

l **Wayfair (sklep meblowy online)**: wayfareblackfriday[.]com

l **SOREL (marka obuwia)**: soreloutletblackfriday[.]com

l **J.Crew (amerykańska marka odzieżowa)**: jcrewblackfriday[.]com

**E-mail phishing: powtarzalne schematy**

Phishing to jedno z głównych narzędzi cyberprzestępców. Fałszywe wiadomości e-mail obiecujące ogromne zniżki w tym roku ponownie kierują użytkowników na niebezpieczne strony. Schematy tych wiadomości są powtarzalne – informacja o „wyjątkowej” promocji, dostępnej tylko teraz, po przejściu na wskazaną stronę internetową. Zmieniają się jedynie nadawcy i linki. Oto przykłady linków ze złośliwych wiadomości:

l **Rolex**: „Zegarki od 250 USD” (np. www[.]hotwatch[.]su)

l **Louis Vuitton**: „Torby z rabatem do 90%” (np. www[.]85off-lvbags[.]com)

**Zagrożenie Ransomware w Handlu Detalicznym**

USA okazuje się najbardziej atakowanym regionem, jeśli chodzi o incydenty ransomware. Ich liczba wzrosła o 24% w porównaniu z zeszłym rokiem. Detaliści w USA stanowią 45% globalnych ataków ransomware na sektor handlu detalicznego, mimo że odpowiadają za mniej niż 30% globalnego rynku detalicznego. Ataki te stanowią poważne zagrożenie dla firm w sezonie świątecznym: mogą zamrozić operacje na długie okresy, nie wspominając o potencjalnie ogromnych karach i odszkodowaniach wynikających z pozwów klientów, których dane wyciekły.

**Jak się chronić?**

Wg specjalistów Check Pointa wystarczą cztery proste kroki, by zminimalizować ryzyko ataku:

1. **Sprawdzaj adres URL i szukaj symbolu kłódki** – Unikaj korzystania z witryn bez szyfrowania SSL (https://).

2. **Ograniczaj dane osobowe** – Nie podawaj numeru PESEL ani daty urodzenia.

3. **Ufaj intuicji** – Zbyt dobre okazje najczęściej są oszustwem.

4. **Używaj kart kredytowych zamiast debetowych** – Oferują lepszą ochronę w przypadku kradzieży.

Dzięki tym środkom ostrożności zakupy w Black Friday mogą być bezpieczne i satysfakcjonujące. Pamiętaj, by korzystać z renomowanych sklepów i zawsze weryfikować autentyczność ofert!