**Zakupy w sieci? Zrób je mądrze!**

**• Liczba witryn phishingowych związanych z handlem elektronicznym, podczas tegorocznego sezonu zakupów online, wzrosła ponad dwukrotnie od listopada 2018 r.**

**• Linki do stron phishingowych są dystrybuowane za pośrednictwem poczty e-mail, w nadziei, że przejdą one niewykryte wśród wielu legalnych ofert rabatowych.**

**• Pokazujemy przykład takiej operacji oszustwa, które podrabia witrynę wiodącej marki okularów, aby przyciągnąć kupujących do podejrzanych zakupów.**

Przygotowania do sezonu świątecznego są w pełnym rozkwicie: dzień singli w Chinach, Święto Dziękczynienia, Czarny piątek i Cyber-poniedziałek są wyróżniającymi się datami w kalendarzu każdego detalisty, którzy próbując zwabić klientów, przygotowują się do internetowych wyprzedaży.

Wynik sprzedaży w dzień singli w „Alibaba” sięgnął 38,4 miliarda USD w ciągu zaledwie 24 godzin, co jest rekordowym wynikiem. W Stanach Zjednoczonych wydatki online w Cybernetyczny poniedziałek mają być również rekordowe, przebijając zeszłoroczny poziom 7,8 miliarda USD!

Jednak nie tylko sklepy i kupujący się przygotowują. Również hakerzy organizują swoją infrastrukturę, aby spróbować wykorzystać część naszych wydatków świątecznych.

W jaki sposób? Jedną z popularnych technik ataku jest zachęcanie kupujących do odwiedzania fałszywych, specjalnie skonstruowanych stron internetowych, które podszywają się pod legalne witryny zakupowe. Cyberprzestępcy mogą następnie ukraść dane karty kredytowej wprowadzone nieświadomie przez użytkowników lub po prostu bezpośrednio skraść pieniądze za pośrednictwem PayPala - bez wysyłania towarów, za które kupujący zapłacili.

**Przestępcy wyłudzają informacje**

W listopadzie 2018 r., byliśmy świadkami znacznego wzrostu liczby stron phishingowych związanych z e-handlem, do których dostęp jest uzyskiwany bezpośrednio lub z linków wysyłanych pocztą elektroniczną. W tym roku możemy zaobserwować podobny trend. **W połowie listopada 2019 – jeszcze przed szczytem Czarnego piątku i Cybernetycznego poniedziałku - użycie adresów phishingowych w e-handlu zwiększyło się o 233% w porównaniu do listopada 2018.**

**Podrób i wykorzystaj**

Pierwszym krokiem do takich operacji jest zarejestrowanie domeny podobnej do znanych, legalnych sklepów internetowych. Domeny to internetowe adresy tekstowe używane do wyszukiwania stron internetowych i usług w Internecie. Muszą być zarejestrowane, a każda ma swojego właściciela. Podrobione sklepy muszą posiadać bardzo podobną domenę do ich prawdziwych odpowiedników, aby uniknąć wzbudzania podejrzeń potencjalnych klientów.

W ciągu ostatnich sześciu miesięcy zarejestrowano ponad 1700 domen, które wyglądają podobnie do domeny amazon.com, np. „Amaz0n-jp [.] Com” ma sprawiać wrażenie autentycznej japońskiej witryny Amazona. Niektóre z tych domen zostaną zapewne wykorzystane do oszukiwania ludzi podczas nadchodzącego sezonu zakupowego.

Pierwszym złośliwym zastosowaniem tych domen są e-maile. Hakerzy będą rozsyłać fałszywe wiadomości, oferując specjalne oferty sprzedaży. Popularne są np. strony oferujące w Czarny piątek rabat do 80% na okulary przeciwsłoneczne Ray Ban.

**Tanie okulary przeciwsłoneczne?**

Kampania rozpoczęła się już 7 listopada i została rozesłana do tysięcy potencjalnych ofiar. Podczas gdy usługi poczty e-mail mają mechanizmy identyfikacji kampanii spamowych na dużą skalę, hakerzy stosują szeroki wachlarz technik w celu obejścia tych filtrów. Na przykład wykorzystują światową sieci zainfekowanych hostów (botów) w celu masowej dystrybucji złośliwych wiadomości e-mail z różnych lokalizacji.

Kliknięcie obrazu w wiadomości otwiera fałszywą witrynę Ray-Ban wyświetlającą wyjątkowe oferty. Witryna używa, podobnej do oryginalnej, domeny **xwrbs[.]com** - **rbs** (Okulary Ray Ban) i umożliwia płatność za pomocą pay-pal. Zamówienie jednak nigdy nie dotrze do odbiorcy, chyba że będą to tanie podróbki.

**Jak uniknąć podobnych prób oszustwa? Check Point zaleca następujące kroki:**

1. Sprawdź, czy zamawiasz z autentycznego źródła. Jednym ze sposobów na to jest NIE klikanie linków promocyjnych i e-maili, a zamiast tego wyszukanie w Google pożądanego sprzedawcy i kliknięcie linku na stronie wyników.

2. Strzeż się „ofert specjalnych”. 80% zniżki na nowy telefon iPhone raczej nie jest godną zaufania okazją do zakupu.

3.

Uważaj na nazwy domen, błędy ortograficzne w wiadomościach e-mail lub witrynach internetowych oraz nieznanych nadawców wiadomości e-mail.