# 1. Rogue WordPress wtyczka ujawnia witryny e-commerce na kradzież kart kredytowych

Łowcy zagrożeń odkryli nieuczciwą wtyczkę WordPress, która jest zdolna do tworzenia fałszywych użytkowników administratora i wstrzykiwania złośliwego kodu JavaScript do kradzieży informacji o karcie kredytowej.

Według Sucuri aktywność przeglądania jest częścią kampanii Magecart skierowanej do witryn e-commerce.

„Podobnie jak w przypadku wielu innych złośliwych lub fałszywych wtyczek WordPress zawiera pewne zwodnicze informacje na górze pliku, aby dać mu okleinę legitymacji” - powiedział badacz bezpieczeństwa Ben Martin.„W tym przypadku komentarze twierdzą, że kod jest„ Dodatkami pamięci podręcznej WordPress ”.

Złośliwe wtyczki zazwyczaj znajdują drogę do witryn WordPress za pośrednictwem zagrożonego użytkownika administratora lub wykorzystania wad bezpieczeństwa w innej wtyczce już zainstalowanej na stronie.

Po instalacji wtyczka replikuje się do katalogu MU-Plugins (lub konieczności wtyczek), aby została automatycznie włączona i ukrywa swoją obecność w panelu administracyjnym.

Odkryj tajne taktyki, które używają hakerzy, aby zostać administratorami, jak wykryć i zablokować, zanim będzie za późno.Zarejestruj się na nasze seminarium już dziś.

„Ponieważ jedynym sposobem na usunięcie któregokolwiek z Mu-Plugins jest ręczne usunięcie pliku, złośliwe oprogramowanie znika, aby temu zapobiec”-wyjaśnił Martin.„Złośliwe oprogramowanie osiąga to, niezarejestrowanie się w funkcjach wywołania zwrotnego dla haczyków, których normalnie używają wtyczki”.

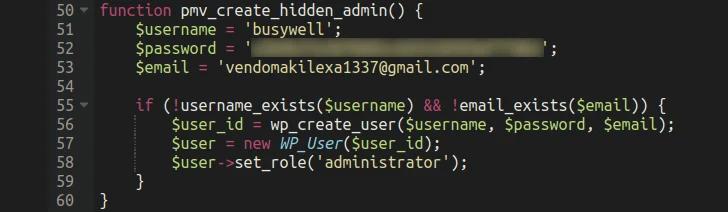
Nieprawidłowa wtyczka jest również wyposażona w opcję, aby utworzyć i ukryć konto użytkownika administratora przed legalnym administratorem witryny, aby uniknąć podniesienia czerwonych flag i utrzymywał dostęp do celu przez dłuższy czas.

Ostatecznym celem kampanii jest wstrzyknięcie karty kredytowej kradzieży złośliwego oprogramowania na stronach kasy i wydłużenie informacji do domeny kontrolowanej przez aktora.

„Ponieważ wiele infekcji WordPress występuje od zagrożonych użytkowników administratora WP-Admin, jest to tylko powód, aby oni musieli pracować w ramach ograniczeń dostępnych, które mają, a instalowanie wtyczek jest z pewnością jedną z kluczowych zdolności, które posiada administrator WordPress- powiedział Martin.

Ujawnienie pojawia się tygodnie po tym, jak społeczność bezpieczeństwa WordPress ostrzegł przed kampanią phishingową, która ostrzega użytkowników o niepowiązanej wadach bezpieczeństwa w systemie zarządzania treścią sieci i nakłada je na instalację wtyczki pod pozorem łatki.Ze swojej części wtyczka tworzy użytkownika administratora i wdraża powłokę internetową do utrzymującego się zdalnego dostępu.

SuSuri powiedział, że aktorzy zagrożeń stojącej za kampanii wykorzystują status „zastrzeżonego” związanego z identyfikatorem CVE, który dzieje się, gdy został zarezerwowany do użytku przez organ ds. Numerowania CVE (CNA) lub badacza bezpieczeństwa, ale szczegóły jeszcze się nie udajewypełniony.



Przychodzi również, gdy firma bezpieczeństwa witryny odkryła kolejną kampanię Magecart, która korzysta z protokołu WebSocket Communications do wstawienia kodu skimmera do sklepów internetowych.Następnie złośliwe oprogramowanie uruchamia się po kliknięciu fałszywego przycisku „Kompletne zamówienie”, który jest nakładany na górę uzasadnionego przycisku kasy.

Raport Spotlight Europola na temat oszustw online opublikowanych w tym tygodniu opisano cyfrowe przeglądanie jako trwałe zagrożenie, które powoduje kradzież, ponowne odsprzedaż i niewłaściwe wykorzystanie danych karty kredytowej.„Główną ewolucją w przeglądaniu cyfrowym jest przejście od wykorzystania złośliwego oprogramowania z front-end do złośliwego oprogramowania, co utrudnia wykrycie”-powiedział.

Unia Europejska.Agencja organów ścigania stwierdziła, że powiadomiła również 443 kupców internetowych, że dane karty kredytowej lub karty płatności ich klientów zostały naruszone za pomocą ataków przeglądających.

Grupa-IB, która współpracowała również z Europolem w zakresie transgranicznej operacji walki z cyberprzestępczością pokonną cyfrową akcję przeglądania, powiedziała i zidentyfikowała 23 rodziny JS-Styffers, w tym Atmzow, Health\_Check, FirstKiss, Fidega, Angrybeaver, Inter i R3nin,które były używane przeciwko firmom w 17 różnych krajach w Europie i Ameryce.

„W sumie 132 rodziny JS-Sniffer jest znane, na koniec 2023 r., Aby skompromitować strony internetowe na całym świecie”-dodała firma o headułach w Singapurze.

To nie wszystko.Wykazano, że fałszywe reklamy w wyszukiwarce Google i Twittera dla platform kryptowalutowych promują drenaż kryptowaluty o imieniu MS Drainer, który, jak się szacuje, już splądrowała 58,98 miliona dolarów od 63 210 ofiar od marca 2023 r. Za pośrednictwem sieci 10 072 witryn phishingowych.

Link: <https://thehackernews.com/2023/12/rogue-wordpress-plugin-exposes-e.html>

# 2. Chameleon Android Banking Variant Trojan omija uwierzytelnianie biometryczne

Badacze cyberbezpieczeństwa odkryli zaktualizowaną wersję złośliwego oprogramowania bankowego z Androidem o nazwie Chameleon, która rozszerzyła celowanie o użytkowników w Wielkiej Brytanii i Włoch.

„Reprezentując restrukturyzowaną i ulepszoną iterację swojego poprzednika, ten rozwinięty wariant kameleon wyróżnia się w realizacji przejęcia urządzeń (DTO) przy użyciu usługi dostępności, a jednocześnie rozszerzając swój ukierunkowany region” - powiedziała holenderska firma zajmująca się ochroną mobilną ThreatFabric.

Chameleon został wcześniej udokumentowany przez Cyble w kwietniu 2023 r., Zauważając, że był używany do wyróżnienia użytkowników w Australii i Polsce od co najmniej stycznia.Podobnie jak inne złośliwe oprogramowanie bankowe, wiadomo, że nadużywa swoich uprawnień do usługi dostępności Androida w celu zebrania wrażliwych danych i przeprowadzania ataków nakładek.

Rogue Apps zawierające wcześniejszą wersję były gospodarzem stron phishingowych i stwierdzono, że podszywają się pod prawdziwe instytucje w krajach, takie jak Australian Taxation Office (ATO) i platforma handlu kryptowalutami o nazwie Coinspot, w celu pożyczenia im wiarygodności.

Najnowsze ustalenia z ThreeadFabric Show, że trojan bankowy jest teraz dostarczany za pośrednictwem Zombinder, gotowego kroplowania-as-usługi (DAAS), który jest sprzedawany innym podmiotom zagrożeniowym i który można wykorzystać do „wiązania” złośliwych ładunkówdo legalnych aplikacji.

Odkryj tajne taktyki, które używają hakerzy, aby zostać administratorami, jak wykryć i zablokować, zanim będzie za późno.Zarejestruj się na nasze seminarium już dziś.

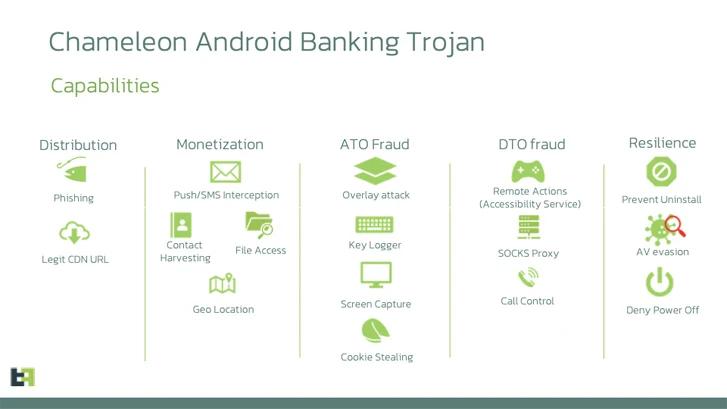
Chociaż podejrzewano, że oferta została zamknięta na początku tego roku, pojawiła się w zeszłym miesiącu, możliwości reklamowe, aby ominąć funkcję „ograniczonych ustawień” w Android w celu zainstalowania złośliwego oprogramowania na urządzeniach i uzyskania dostępu do usługi dostępności.

Oba złośliwe artefakty dystrybuujące maskaradę kameleon jako przeglądarka internetowa Google Chrome.Ich nazwy pakietów są wymienione poniżej -

Z72645C414CE232F45.Z35AAD4DDE2FF09B48

com.busy.lady

Godną uwagi cechą ulepszonego wariantu jest jego zdolność do przeprowadzania oszustwa przejęcia urządzeń (DTO), która wykorzystuje usługę dostępności do wykonywania nieautoryzowanych działań w imieniu ofiary.



Ale aby oszukać użytkowników, aby umożliwić ustawienie, złośliwe oprogramowanie sprawdza wersję Androida na zainstalowanym urządzeniu, a jeśli okaże się, że jest Android 13 lub nowszy, zachęca użytkownika do włączenia go.

„Po otrzymaniu potwierdzenia systemu Androida 13 ograniczonych ustawień na zainfekowanym urządzeniu, trojan bankowy inicjuje ładowanie strony HTML”, wyjaśnił ThreatFabric.„Strona prowadzi użytkowników poprzez ręczny proces krok po kroku, aby umożliwić usługę dostępności na Androida 13 i wyższej”.

Kolejnym nowym dodatkiem jest użycie interfejsów API z Androidem do zakłócenia operacji biometrycznych docelowego urządzenia poprzez potajemne przejście mechanizmu uwierzytelniania ekranu blokady na PIN, aby umożliwić złośliwemu oprogramowaniu „odblokowanie urządzenia w Will” przy użyciu usługi dostępności.

„Pojawienie się nowego trojana bankowego Chameleon jest kolejnym przykładem wyrafinowanego i adaptacyjnego krajobrazu zagrożenia w ekosystemie Androida” - powiedziała firma.„Ewoluując od wcześniejszej iteracji, ten wariant pokazuje zwiększoną odporność i zaawansowane nowe funkcje”.

Rozwój pojawia się, gdy Zimperium ujawniło, że 29 rodzin złośliwego oprogramowania - 10 nowych - w ciągu ostatniego roku miało na celu 1800 aplikacji bankowych w 61 krajach.Nowe aktywne rodziny to Nexus, Ojciec chrzestny, Pixpirate, Saderat, Hook, Pixbankbot, Xenomorph V3, Vultur, Brasdex i Goatrat.

Krajowe kraje USA obejmują USA (109 aplikacji bankowych), Wielka Brytania (48), Włochy (44), Australia (34), Turcja (32), Francja (30), Hiszpania (29), Portugalia (27),Niemcy (23), Kanada (17) i Brazylia (11).Najbardziej ukierunkowane aplikacje usług finansowych to Phonepe (Indie), WeChat, Bank of America, Well Fargo, (U.S.), Binance (Malta), Barclays (Wielka Brytania), QNB Finansbank (Turcja) i Caixabank (Hiszpania).

Link: <https://thehackernews.com/2023/12/new-chameleon-android-banking-trojan.html>