Domeny ZIP jako fałszywe

Google postanowiła udostępnić możliwość rejestracji domen .zip, ale jest też łatwym kąskiem dla przestępców.

Domeny ZIP łatwy kąsek dla przestępców

Cyberprzestępcy będą wykorzystywać je w swoich kampaniach phishingowych, kreatywnie podsuwając internautom złośliwe adresy URL i rozpowszechniając złośliwe oprogramowanie.

Powstała również wcześniej taka domena jak „microsoft-office.zip – służąca do kradzieży danych logowania do kont Microsoft, ale Google zdążył ją już w miarę szybko usunąć.

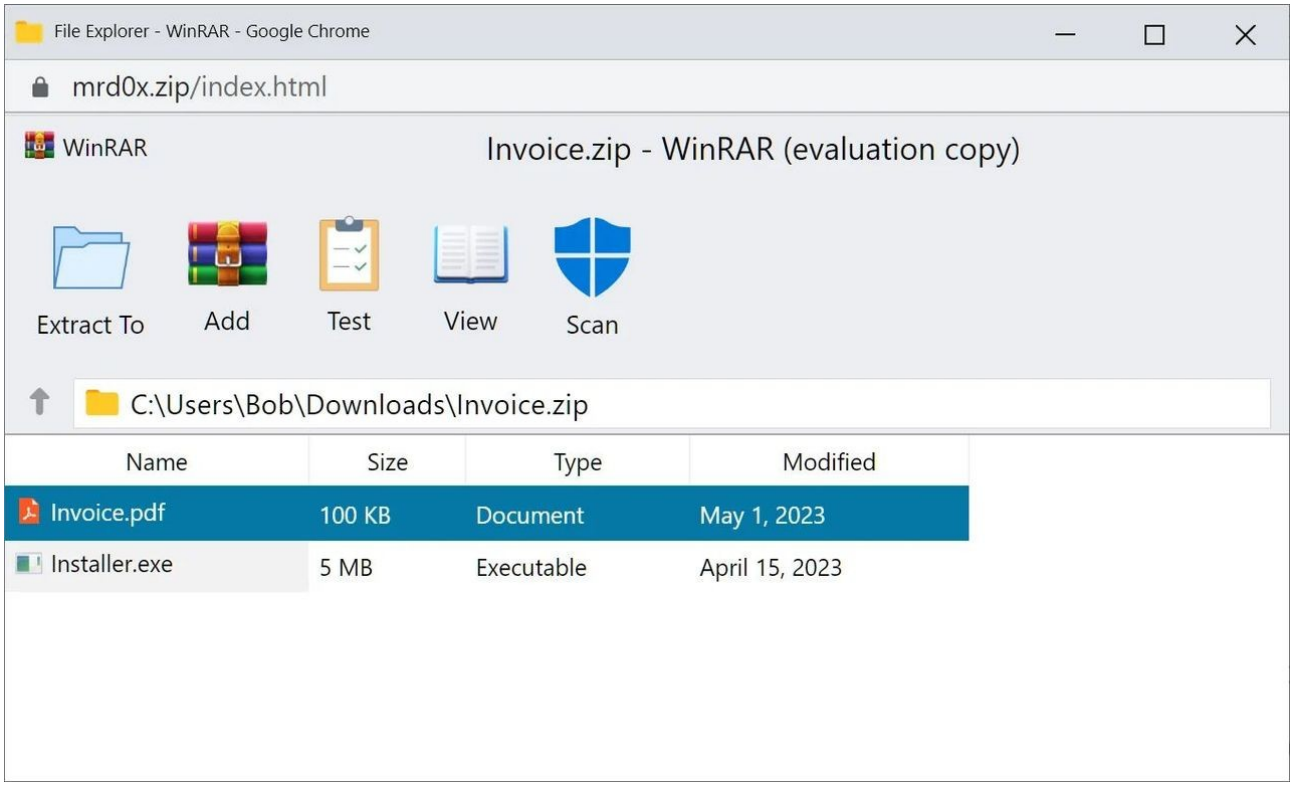
Szczerze to trochę średnie posunięcie ze strony giganta „Google" umożliwiając rejestrację domen .zip, gdyż mogą być nieprzewidziane konsekwencje (chodzi o wirusy, rozprzestrzenianie ich).

Narzędzie do identyfikacji stron .zip

Badacz bezpieczeństwa – mr.d0x opracował dość interesujące, a niezwykle pomocne narzędzie do phishingu, pozwalający na otwieranie fałszywych instancji WinRAR oraz Eksploratora plików bezpośrednio z przeglądarki.

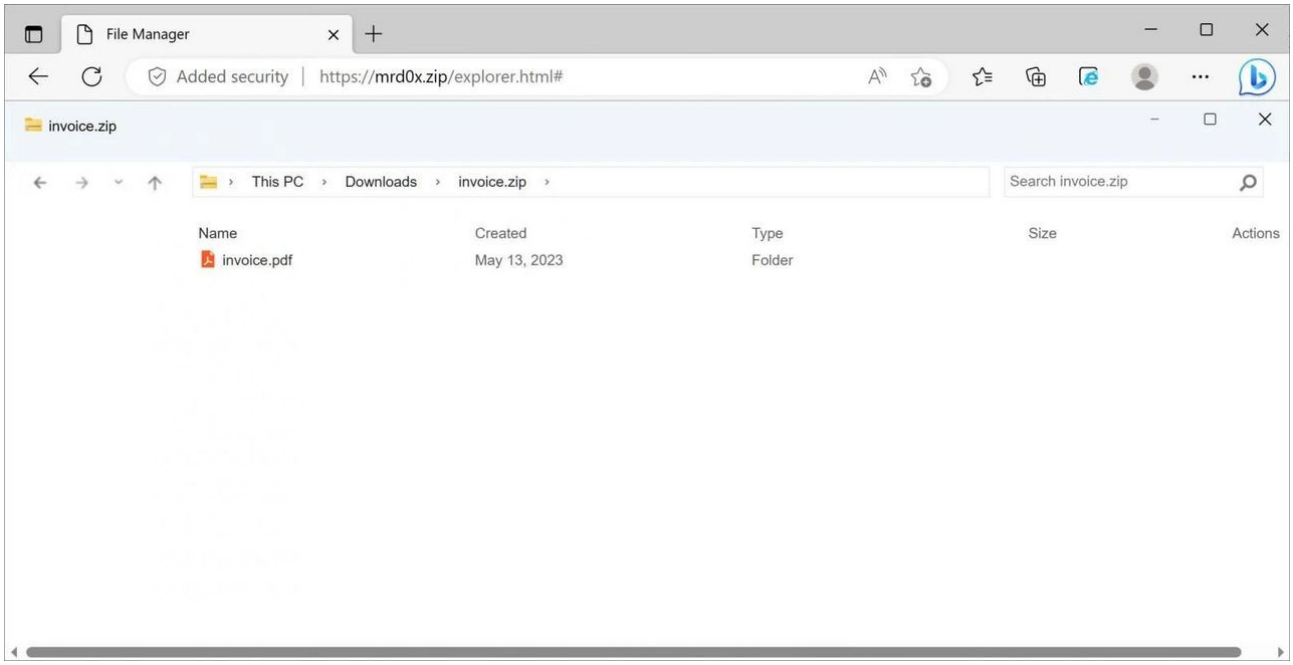
To wszystko jest wyświetlane w domenach ZIP. Wszystko po to, by oszukać użytkowników w taki sposób, aby myśleli, że otwierają plik ".zip". Jak tłumaczy sam specjalista: „*Dzięki temu atakowi phishingowemu symulujesz oprogramowanie do archiwizacji plików (np. WinRar) w przeglądarce i*

używasz domeny .zip, aby wyglądała na bardziej wiarygodną”



Demonstracja zawiera zestaw narzędzi, który może zostać użyty do osadzenia fałszywego okna WinRar bezpośrednio w przeglądarce. Gdy otwierana jest domena .zip, efekt wygląda następująco, jakby użytkownik otworzył archiwum ZIP i teraz widział zawarte w nim pliki.

Aby fałszywe okno WinRar było jeszcze bardziej przekonujące, naukowcy zaimplementowali fałszywy przycisk Skanuj, który po kliknięciu mówi, że pliki zostały przeskanowane i nie wykryto żadnych zagrożeń.



Specjalista mr.d0x stworzył również fałszywy „Eksplorator plików Windows” udający, że otwiera plik .zip. Jak sami widzicie brakuje w nim niektórych elementów, ponieważ to wszystko jest jeszcze w fazie rozwojowej.

Jak dochodzi do wyłudzeń danych?

mr.d0x wyjaśnia, że taki zestaw narzędzi phishingowych jest stosowany zarówno do kradzieży danych uwierzytelniających jak i zarówno do przesyłania złośliwego oprogramowania.

Np. jeśli dwukrotnie klikniemy w plik PDF w fałszywym oknie WinRar czy tam 7-zip, to zostaniemy przekierowani zupełnie na inną stronę. Może być prośba bynajmniej o podanie danych logowania (w celu autoryzacji pliku).