Bitdefender

Badacze odkrywają „MalDoc w formacie PDF” – nową technikę cyberprzestępców

05.09.2023

Badacze zajmujący się cyberbezpieczeństwem z JPCERT/CC zaprezentowali nowatorską i wyrafinowaną technikę omijania systemów antywirusowych o nazwie „MalDoc in PDF”. Odkrycie to wynikło z dochodzenia w sprawie ataku, który miał miejsce w lipcu 2023 r. Dlatego zespół Bitdefender przygotował artykuł, w którym wyjaśnia, czym jest MalDoc w formacie PDF i w jaki sposób użytkownik sieci może się przed nim uchronić.

Co to jest MalDoc w formacie PDF?

Według Yumy Masubuchi i Kota Kino, badaczy, którzy dokonali odkrycia złośliwego oprogramowania, „plik utworzony w programie MalDoc w formacie PDF można otworzyć w programie Word, mimo że zawiera „magiczne” liczby i strukturę pliku PDF. Jeśli plik ma skonfigurowane

makro, otwierając go w programie Word VBS działa i wykonuje złośliwe zachowania. W ataku potwierdzonym przez JPCERT/CC rozszerzenie pliku zawierał sufiks .doc. Dlatego też, jeśli plik .doc jest skonfigurowany do otwierania w programie Word w ustawieniach systemu Windows, plik utworzony przez MalDoc w formacie PDF zostanie on otwarty przez Word."

Dylemat poligloty

Pliki wykazujące takie zachowanie nazywane są poliglotami, czyli legalnymi formami wielu typów plików. W tym przypadku poliglota MalDoc w formacie PDF naśladuje zarówno pliki PDF, jak i DOC (Word). Cyberprzestępcy osiągają to za pomocą pliku MHT utworzonego w programie Word z makrem dołączonym do obiektu pliku PDF.

Spowoduje to utworzenie pliku, który wygląda na prawidłowy plik PDF, ale można go również otworzyć w programie Word. Po otwarciu jako DOC w pakiecie Microsoft Office plik uruchamia makra VBS przeznaczone do pobierania i wdrażania plików złośliwego oprogramowania MSI.

Wyzwanie wykrywania

Tradycyjne narzędzia do analizy plików PDF pdfid mogą nie rozpoznawać złośliwych składników takich plików. Zdaniem badaczy ze względu na dwoistość pliku utworzonego za pomocą programu MalDoc w formacie PDF analiza go przy użyciu tradycyjnych narzędzi może nie ujawnić jego szkodliwych składników.

Chociaż niektóre narzędzia wyposażone w odpowiednie moduły, np. zdolność narzędzi do analizy plików programu Word OLEVBA mogą posłużyć do wykrywania makr osadzonych w tych fałszywych dokumentach, to technika ta nadal stwarza poważne wyzwania.

Pocieszające jest to, że podobna metoda wykorzystująca pliki Excel spowodowała wyświetlenie komunikatu ostrzegawczego, ostrzegającego użytkownika o ryzyku.

Implikacje i środki ostrożności

Choć MalDoc w formacie PDF nie omija ustawień wyłączających automatyczne wykonywanie makr programu Word, technika ta może w dalszym ciągu oszukać niektóre systemy antywirusowe, które będą charakteryzowały ten złośliwy plik jako zwykły PDF. Podkreśla to potrzebę ciągłej czujności i zaawansowanych metod wykrywania, aby przeciwdziałać stale ewoluującej taktyce cyberprzestępców.

„Ponieważ eksperci ds. cyberbezpieczeństwa szukają rozwiązania problemu MalDoc w formacie PDF, użytkownikom zaleca się zachowanie ostrożności podczas otwierania nieznanych plików DOC lub PDF oraz regularne aktualizowanie oprogramowania antywirusowego” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Na razie złośliwe oprogramowanie wdrażane za pomocą tej techniki pozostaje niezidentyfikowane, ale dochodzenie ekspertów do spraw

cyberbezpieczeństwa jest kontynuowane i wkrótce spodziewane są aktualizacje.

Źródło: https://bitdefender.pl/badacze-odkrywaja-maldoc-w-formacie-pdf-nowa-technike-cyberprzestepcow/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 05.09.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.