Bitdefender

Różnice między statyczną i dynamiczną analizą złośliwego oprogramowania

30.08.2023

W miarę jak ludzie i firmy stają się coraz bardziej uzależnieni od technologii, złośliwe oprogramowanie tym samym staje się coraz większym zagrożeniem zarówno dla organizacji, jak i osób prywatnych. Jednocześnie nowe technologie ułatwiają przestępcom tworzenie nowego szkodliwego oprogramowania. Aby chronić się przed rosnącym zagrożeniem, specjaliści ds. cyberbezpieczeństwa wykorzystują analizę złośliwego oprogramowania do wykrywania cech i możliwości niebezpiecznych programów. Pozwala im to zrozumieć zagrożenia, jakie stwarzają te programy, oraz opracować mechanizmy obronne, a także środki zaradcze, które pomogą im złagodzić konsekwencje potencjalnych ataków. Istnieją dwa rodzaje technik analizy złośliwego oprogramowania — statyczne i dynamiczne. Poniżej zespół Bitdefender przedstawi różnice między tymi dwiema technikami oraz zbadajmy ich mocne i słabe strony.

Czym jest analiza złośliwego oprogramowania?

Analiza złośliwego oprogramowania to inspekcja głównych komponentów i kodu źródłowego złośliwego oprogramowania w celu zrozumienia jego zachowania, pochodzenia oraz zamierzonych działań w celu ograniczenia potencjalnych zagrożeń.

Złośliwe oprogramowanie oznacza każde natrętne oprogramowanie zaprojektowane w celu infiltracji komputera lub sieci użytkownika bez jego zgody. Do takich niebezpiecznych plików zaliczają się programy szpiegujące, scareware, rootkity, robaki, wirusy i konie trojańskie.

Złośliwe programy można zaprogramować tak, aby kradły dane użytkowników, szpiegowały ich działania online, a nawet uszkadzały pliki systemowe. Przykładowo na początku stycznia 2023 r. w firmie Pepsi Bottling Ventures doszło do naruszenia bezpieczeństwa danych, gdy do jej sieci przedostało się złośliwe oprogramowanie kradnące dane osobowe.

Statyczna analiza złośliwego oprogramowania

W przypadku statycznej analizy złośliwego oprogramowania eksperci ds. bezpieczeństwa analizują szkodliwy program bez wykonywania jego kodu. Celem jest identyfikacja rodzin złośliwego oprogramowania, sposobu działania szkodliwego kodu i jego możliwości.

Statyczna analiza złośliwego oprogramowania nie wymaga środowiska

na żywo. Może to jednak spowodować, że analitycy przeoczą najważniejsze informacje na temat szkodliwego oprogramowania, które można wykryć, jedynie obserwując jego działanie.

Oto kilka charakterystycznych cech statycznej analizy złośliwego oprogramowania.

Jest szybka i prosta

Analiza statyczna jest prosta, ponieważ eksperci muszą jedynie ocenić właściwości próbki złośliwego oprogramowania, takie jak metadane, ciągi znaków, struktura i kod.

Ponieważ analitycy nie muszą wykonywać kodu, mogą szybko zidentyfikować funkcjonalność i możliwości szkodliwego oprogramowania. Można go również zautomatyzować za pomocą narzędzi takich jak dezasemblery, dekompilatory i debugery, aby szybko analizować dużą liczbę próbek złośliwego oprogramowania.

Jest oparty na podpisie

Statyczna analiza złośliwego oprogramowania wykorzystuje metodę wykrywania opartą na sygnaturach, która porównuje cyfrowy ślad przykładowego kodu z bazą danych zawierającą znane sygnatury złośliwych programów. Każde złośliwe oprogramowanie ma unikalny cyfrowy odcisk palca, który jednoznacznie go identyfikuje. Może to być skrót kryptograficzny, wzór binarny lub ciąg danych.

Programy antywirusowe działają w ten sam sposób. Skanują dysk w poszukiwaniu złośliwego oprogramowania, przeglądając cyfrowe ślady znanych sygnatur złośliwego oprogramowania i oznaczają plik jako złośliwe oprogramowanie, jeśli skanowanie wykryje pasujące ślady.

Chociaż metoda analizy złośliwego oprogramowania oparta na sygnaturach jest skuteczna w wykrywaniu znanych sygnatur złośliwego oprogramowania, zawodzi ona w przypadku nowego lub zmodyfikowanego złośliwego oprogramowania.

Metoda ta może równie nie wykryć próbek złośliwego oprogramowania zaprogramowanego do aktywacji tylko w określonych warunkach, takich jak te wywołane przez dziennik użytkownika, datę, godzinę lub ruch sieciowy.

Stosowane techniki podczas analizy statycznej

Statyczna analiza złośliwego oprogramowania wykorzystuje różne techniki, aby zrozumieć naturę zagrożenia. Jedno podejście polega na porównaniu cyfrowego odcisku palca pliku binarnego złośliwego oprogramowania z dostępnymi bazami danych zawierającymi złośliwe sygnatury.

Technik może również użyć dezasemblera lub debugera do przeprowadzenia inżynierii wstecznej pliku binarnego w celu sprawdzenia jego kodu. Alternatywnie niektórzy analitycy przeprowadzają statyczną analizę złośliwego oprogramowania, wyodrębniając metadane w postaci ciągu znaków. Spowoduje to

ujawnienie szczegółów, takich jak polecenia, nazwy plików, komunikaty, wywołania API, klucze rejestru, adresy URL i inne IOC.

Dynamiczna analiza złośliwego oprogramowania

Dynamiczna analiza złośliwego oprogramowania obejmuje wykonanie kodu złośliwego oprogramowania w kontrolowanym środowisku i monitorowanie jego interakcji z systemem. Taka analiza pozwala analitykom odkryć prawdziwe intencje szkodliwego oprogramowania i jego zdolność do uniknięcia wykrycia.

Podejście to zapewnia bardziej szczegółowy i dokładny raport, ale proces może potrwać dłużej. Wymaga również specjalistycznych narzędzi i istnieje ryzyko zainfekowania środowiska analitycznego złośliwym oprogramowaniem.

Dynamiczna analiza złośliwego oprogramowania charakteryzuje się tym, że:

Wymaga piaskownicy

Aby bezpiecznie uruchomić złośliwe oprogramowanie i obserwować jego działania, analitycy bezpieczeństwa potrzebują zamkniętego środowiska testowego (piaskownicy złośliwego oprogramowania), w którym złośliwe oprogramowanie może działać bez infekowania całego systemu lub sieci.

Jest bardziej wszechstronne i dokładne

Analiza dynamiczna jest uważana za dokładniejszą i wszechstronniejszą niż analiza statyczna, ponieważ obejmuje głęboką analizę zachowania.

Obserwując, jak podejrzany plik wykonuje każde ze swoich poleceń, analitycy mogą uzyskać głęboki wgląd w logikę, funkcjonalność i wskaźniki naruszenia bezpieczeństwa szkodliwego oprogramowania. Innymi słowy, pokazuje rzeczy, które trudniej jest stwierdzić na podstawie analizy statycznej, takie jak to, do czego zaprogramowano szkodliwe oprogramowanie, w jaki sposób się komunikuje i jakie są jego mechanizmy unikania.

Opiera się na zachowaniu aplikacji

Podczas gdy analiza statyczna wykorzystuje wykrywanie na podstawie sygnatury, analiza dynamiczna wykorzystuje podejście do wykrywania w oparciu o zachowanie. Szybko rozwijające się złośliwe oprogramowanie lub nowe typy złośliwego oprogramowania mogą być trudne do wykrycia przy użyciu podejścia opartego na sygnaturach. Niektóre formy złośliwego oprogramowania mogą również ukrywać swój podpis, przez co analiza statyczna staje się nieskuteczna.

Ponieważ analiza dynamiczna wykorzystuje podejście do wykrywania opartego na zachowaniu, zapewnia analitykom bezpieczeństwa identyfikację i zrozumienie nowych i nieznanych zagrożeń.

Biorąc pod uwagę, że rynek sztucznej inteligencji będzie rósł o ponad 38% rocznie w latach 2022–2029, możemy spodziewać się wzrostu

liczby nowego złośliwego oprogramowania za pośrednictwem platform opartych na sztucznej inteligencji, takich jak ChatGPT. Dynamiczna analiza złośliwego oprogramowania będzie odgrywać kluczową rolę w pomaganiu analitykom bezpieczeństwa w zrozumieniu nowo pojawiających się zagrożeń.

Stosowane techniki podczas analizy dynamicznej

Niektóre z technik stosowanych podczas dynamicznej analizy złośliwego oprogramowania obejmują:

Monitorowanie aktywności: technika ta polega na monitorowaniu wywołań systemowych wykonywanych przez złośliwe oprogramowanie podczas działania, takich jak tworzenie lub modyfikowanie plików, otwieranie połączeń sieciowych i wprowadzanie zmian w rejestrze.

Analizę ruchu sieciowego: złośliwe oprogramowanie często kontaktuje się ze zdalnymi serwerami w celu otrzymania poleceń lub wydobycia danych. Analiza ruchu sieciowego polega na monitorowaniu ruchu szkodliwego oprogramowania podczas jego działania, aby poznać serwery, z którymi się komunikuje, rodzaje otrzymywanych poleceń i dane, które wydobywa.

Dynamiczną analizę kodu: technika ta polega na śledzeniu przepływu wykonywania złośliwego oprogramowania, aby zrozumieć, jak działa.

Analizę pamięci: złośliwe oprogramowanie często próbuje ukryć swoje działania w pamięci, na przykład szyfrując dane lub stosując techniki

drążenia procesów. Analitycy wykorzystują analizę pamięci do sprawdzania zawartości pamięci systemowej podczas i po uruchomieniu złośliwego oprogramowania, aby zidentyfikować wszelkie ukryte działania.

Ponieważ zagrożenie ataku złośliwym oprogramowaniem stale rośnie, ważne jest zrozumienie różnic między statyczną i dynamiczną analizą, aby zbudować skuteczne strategie obrony przed zagrożeniami ze strony złośliwego oprogramowania.

„Obie techniki mają swoje mocne i słabe strony, a wybór właściwej dla danej firmy będzie zależał od konkretnych okoliczności analizy zespołu do spraw cyberbezpieczeństwa. Analiza statyczna zapewnia szybkie i skuteczne wyniki poprzez sprawdzenie kodu i struktury złośliwego oprogramowania. Z kolei analiza dynamiczna zapewnia dogłębne spostrzeżenia poprzez obserwację złośliwego oprogramowania działającego w kontrolowanym środowisku i obserwowanie jego zachowania” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Łącząc te techniki, zespoły ds. bezpieczeństwa mogą lepiej zrozumieć zagrożenia stojące za złośliwym oprogramowaniem i opracować skuteczniejsze strategie obrony w celu wykrywania oraz łagodzenia potencjalnych ataków.

Źródło: https://bitdefender.pl/roznice-miedzy-statyczna-i-dynamiczna-analiza-zlosliwego-oprogramowania/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 30.08.2023

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.