MADE IN GERMANY

G DATA BEAST

Przezwyciężanie ograniczeń tradycyjnego wykrywania złośliwego oprogramowania.

Spis treści

Zaawansowane złośliwe oprogramowanie stało się trudne do wykrycia przez tradycyjne metody detekcji oparte o sygnatury.

Ograniczenie nr 1: wykrywanie wsteczne

Po pierwsze i najważniejsze: wykrywanie zagrożeń oparte na sygnaturach jest z definicji metodą reaktywną. Niezależnie od poziomu automatyzacji: tylko po sklasyfikowaniu pliku jako złośliwy można stworzyć sygnaturę dla tego pliku lub grupy powiązanych plików (zazwyczaj rodziny złośliwego oprogramowania).

Dzisiaj twórcy złośliwego oprogramowania przełamują reaktywne podejście przez masowe rozpowszechnianie wirusów, które są postrzegane jako nowe.

Ograniczenie nr 2: unikalność złośliwego oprogramowania

Cyberprzestępczość stała się branżą wartą miliardy dolarów. Podobnie jak tradycyjne firmy, cyberprzestępcy zwiększają swoją wydajność, korzystając z narzędzi automatyzacji. Niektórzy autorzy szkodliwego oprogramowania korzystają z nich do aktywnego monitorowania, czy rozwiązania antywirusowe wykrywają ich złośliwe oprogramowanie. Po zarejestrowaniu wykrycia natychmiast usuwają zidentyfikowany wzór z próbek lub zmieniają kod, aby uniknąć wykrycia.

Aby skomplikować problem stosują także silne algorytmy szyfrowania oraz pakery w celu zaciemnienia złośliwego kodu. Niektórzy twórcy szkodliwego oprogramowania wprowadzają nowe próbki wirusów co kilka minut. Inni generują indywidualne próbki dla każdej pojedynczej ofiary ("server-side polymorphy").

Oczywiście, gdy złośliwe pliki są unikalne, trudno jest znaleźć taki wzorzec, który można byłoby użyć do wygenerowania sygnatur zdolnych do wykrycia całej rodziny złośliwego oprogramowania. Nawet jeśli istnieją wzorce, które można wykorzystać do stworzenia sygnatur, wysiłek ten może być bezcelowy.

Ograniczenie nr 3: unikanie analizy kodu

Innym problemem jest to, że identyfikacja złośliwych plików często opiera się na zapleczu analitycznym producentów zabezpieczeń. Potencjalnie złośliwe próbki, które otrzymują twórcy antywirusów są dokładnie analizowane, na przykład w izolowanych systemach - tzw. piaskownicach (ang. sandbox), w celu identyfikacji złośliwych procesów. Tylko wtedy, gdy próbki zostaną zidentyfikowane jako złośliwe, antywirus zacznie znajdować złośliwe wzorce. Niestety, często próbki szkodliwego oprogramowania są zaprojektowane tak, aby były świadome swojego środowiska i wykrywały czy są analizowane. Mogą ujawniać swoje złośliwe zachowanie tylko w określonym czasie, w określonej lokalizacji lub po rozpoznaniu pewnych działań użytkownika, która zwykle nie występują podczas analizy w piaskownicy.

Z powodu tych problemów oprócz tradycyjnych metod detekcji konieczne jest wykrywanie złośliwego zachowania tam, gdzie może to się wydarzyć: w systemie użytkownika.

Rozwiązanie: analiza zachowania

Aby przeciwdziałać tak zaawansowanym zagrożeniom, dostawcy zabezpieczeń wdrażają technologie, które analizują zachowanie procesów w systemach. Analiza jest skoncentrowana szczególnie na podejrzanych obszarach, takich jak system plików, rejestr lub folder autostartu. Umożliwia to wykrywanie całkowicie nieznanych rodzin złośliwego oprogramowania.

Większość z tych rozwiązań próbuje przełożyć groźne zachowanie na liczbowe wartości, aby określić stopień zagrożenia. Stosując taki model, łatwo jest jednak o błąd, zwłaszcza, gdy wiele z tych wartości jest agregowanych w łączny wynik. Nawet stosując uczenie maszynowe istnieje pewien poziom niepewności w ocenie czy dany proces jest złośliwy, czy bezpieczny.

Większość użytkowników domowych nie zostanie dotknięta tym problemem. W przypadku firm, które zazwyczaj korzystają z wysoce nietypowego, wyspecjalizowanego oprogramowania, pewne procesy mogą wzbudzić metody obronne antywirusa, jeżeli próg narzędzia analizy behawioralnej zostanie ustawiony zbyt wysoko. Natomiast jeśli próg będzie zbyt niski, to złośliwe oprogramowanie może nie zostać wykryte. W prawdziwym świecie dostawcy zabezpieczeń zwykle unikają błędów wykrywania, prosząc użytkownika systemu o ostateczną decyzję. W praktyce, gdy takich zapytań pojawia się zbyt wiele, użytkownicy albo wyłączą ochronę albo zignorują ostrzeżenia. Tak czy inaczej - ryzyko infekcji wzrośnie.

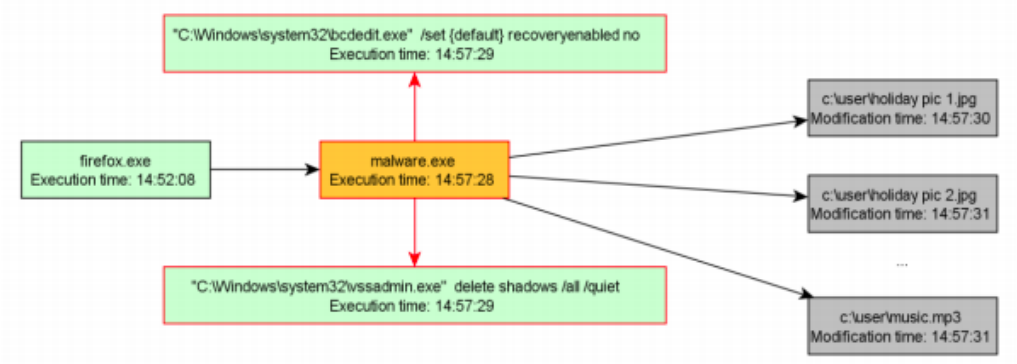
The real solution: BEAST

BEAST jest technologią wykrywania opartą na zachowaniu, opracowaną przez G DATA, która monitoruje zachowanie systemu i przechowuje każde zaobserwowane działanie pod postacią grafu w lokalnej lekkiej bazie danych. Działanie BEAST nie polega na identyfikacji złośliwych plików samych w sobie, ale na obserwacji złośliwych wzorców zachowań i ich powiązań. Jest to szczególnie pomocne w przypadku rzadkiego szkodliwego oprogramowania i rodzin złośliwego oprogramowania.

Jak działa BEAST: dopasowywanie reguł oparte na grafach

W chronionym systemie, BEAST monitoruje zachowanie procesów i przechowuje każdą akcję. Działania obejmują dostęp do systemu plików, rejestru, połączeń sieciowych oraz komunikację między procesami. Ilekroć coś jest dodawane do bazy danych grafów, jest on przeszukiwany pod kątem wzorców zachowań złośliwego oprogramowania.

Poniższy graf może służyć do zilustrowania tego rodzaju dopasowywania opartego na regułach:



Ten użytkownik prawdopodobnie został oszukany przez witrynę internetową w celu pobrania i uruchomienia złośliwego pliku „malware.exe" z Internetu przy użyciu przeglądarki Firefox. W tym przypadku jest to infekcja wirusem typu ransomware. Działanie ransomware polega na szyfrowaniu plików użytkownika, a następnie domaganiu się okupu za odzyskanie danych.

Złośliwy proces natychmiast uruchomił instancję narzędzia systemowego „bcdedit" w celu wyłączenia funkcji naprawy przy uruchomieniu systemu Windows. Następnie uruchomił instancję narzędzia systemowego „vssadmin", aby usunąć kopie zapasowe (volume shadow copy), które można użyć do przywrócenia nadpisanych plików. Następnie rozpoczął szyfrowanie kilku plików w katalogu „C:\user".

Ponieważ uruchomienie dwóch wyżej wymienionych narzędzi systemowych jest typowym przygotowaniem oprogramowania ransomware przed zaszyfrowaniem plików, zachowanie (na wykresie zaznaczone na czerwono) można uznać za wyraźnie złośliwe. Dlatego proces „malware.exe" zostałby zatrzymany, a plik binarny zostałby przeniesiony do kwarantanny. Ponieważ pliki binarne „vssadmin.exe" i „bcdedit.exe" są narzędziami systemowymi użytymi w tym wypadku przez oprogramowanie ransomware, pozostałyby nienaruszone w systemie.

Nowe możliwości: usuwanie retrospektywne

G DATA, przy pomocy automatycznej lub ręcznej analizy procesów, codziennie identyfikuje wiele wskaźników informujących o kompromitacji systemu (IOC). IOC może być serwerem Command&Control (C&C) używanym do obsługi botnetu lub określonym plikiem, który został zidentyfikowany jako złośliwy.

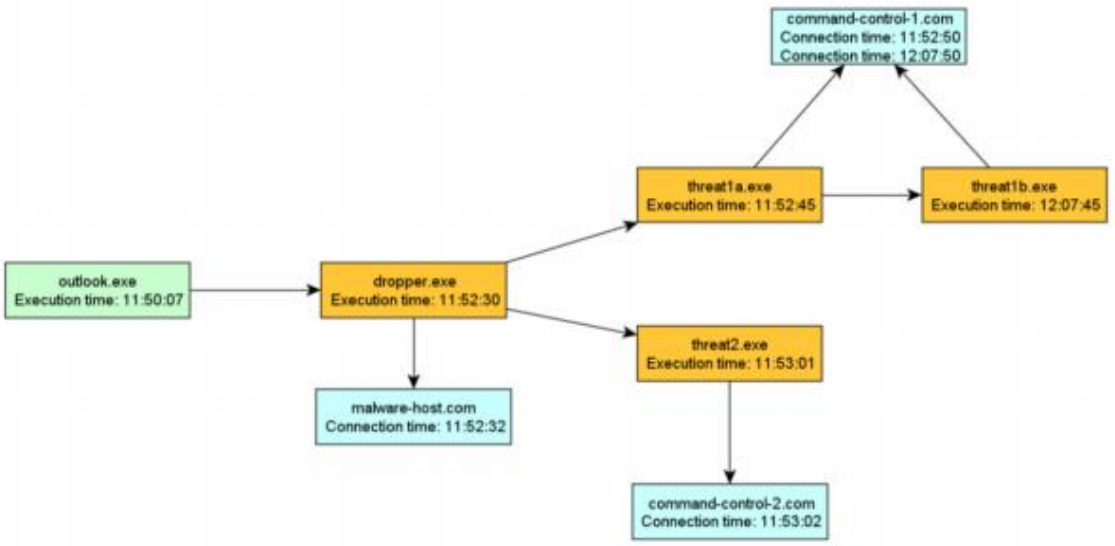
W konwencjonalnych narzędziach ochrony punktów końcowych, akcje są porównywane tylko z listami IOC w momencie wystąpienia zdarzenia. Na przykład, zanim plik zostanie uruchomiony, jest on porównywany z listą znanych złośliwych plików. Innym przykładem jest próba nawiązania połączenia procesu z danym hostem - host jest sprawdzany czy nie znajduje się na liście znanych serwerów C&C. Jeśli host zostanie zidentyfikowany jako złośliwy, to cały proces zostanie zidentyfikowany jako złośliwy.

Podstawowym problemem jest jednak to, że mechanizmy identyfikacji IOC dostawców zabezpieczeń są ponownie reaktywne - rozpoczynają się po tym, jak dostawcy zaczną analizować zagrożenie, co oczywiście może nastąpić dopiero po pojawieniu się zagrożenia. Nawet jeśli jest to zautomatyzowane i wykonane w bardzo krótkim czasie, przerwa czasowa jest nadal znacząca w kontekście wykrywania złośliwego oprogramowania. Mówiąc wprost: producenci zabezpieczeń często działają zbyt późno i jest to jedyne co mogą zrobić, gdy polegają wyłącznie na tradycyjnych metodach wykrywania złośliwego oprogramowania.

W BEAST akcje (zachowania) są przechowywane w lokalnej bazie danych grafów. Dlatego wszystko w tej bazie danych można porównać do IOC zidentyfikowanych przez G DATA, nawet po wystąpieniu tychże akcji. Ponieważ baza danych grafów zawiera również wszystkie działania związane z IOC, wszystkie te działania można cofnąć, co skutecznie umożliwia retrospektywne usunięcie złośliwego oprogramowania.

Jest to szczególnie ważne w momencie, gdy system został przejęty, ale nie zostały jeszcze uruchomione żadne złośliwe procesy, które mogłyby zostać wykryte przez kontrolę zachowania.

Spójrz na poniższy przykład grafu:



Początkowo w programie pocztowym Outlook został uruchomiony zainfekowany załącznik. W związku z tym powstał plik o nazwie "dropper.exe", stworzony przez proces "outlook.exe". Nowy proces nawiązał połączenie z „malware-host.com” w celu pobrania i uruchomienia dalszych złośliwych plików binarnych („threat1a.exe”, „threat2.exe”). Oba połączyły się z odpowiednimi serwerami C&C („command-control-1.com”, „command-control-2.com”). Po około 15 minutach „threat1a.exe” otrzymał polecenie zaktualizowania pliku binarnego do „threat1b.exe”, który z kolei ustanowił połączenie z tym samym serwerem C&C.

Gdy G DATA zidentyfikuje serwer „command-control-2.com” lub plik „dropper.exe” jako IOC, BEAST może - nawet kilka godzin po infekcji - po prostu przeanalizować wykres, a następnie znaleźć i usunąć każdy pojedynczy plik binarny powiązany z infekcją.

Dwie dodatkowe uwagi: Po pierwsze, każda zmiana w rejestrze systemu Windows, a zatem konfiguracja systemu została rejestrowana i aby ją przywrócić (pominięto to na wykresie, aby był bardziej czytelny). Po drugie, program outlook.exe jako znany bezpieczny plik wykonywalny nie został usunięty.

Jaka jest różnica w stosunku do istniejącego modułu Kontroli zachowania?

Istniejący moduł Kontroli zachowania zasadniczo rejestruje strumień akcji wywołanych przez proces. Każdej akcji przypisuje określoną wartość liczbową „złośliwości”. Następnie podsumowuje wszystkie wartości, a gdy pewien próg zostanie przekroczony, proces jest uważany za złośliwy.

Zasadniczo Kontrola zachowania analizuje dany proces, podczas gdy BEAST analizuje cały system operacyjny. Ponadto, ponieważ Kontrola zachowania agreguje tylko liczbowe wartości złośliwych działań, nie można wykryć pewnych kombinacji działań jako złośliwych. Utrudnia to szczególnie wykrycie wzorców złośliwych zachowań. Ilekroć akcja ma przypisaną nową lub wyższą wartość złośliwości w module Kontroli zachowania, może to wywołać fałszywe alarmy (tzw. false positive). To sprawiało, że w przeszłości kłopotliwe było szybkie reagowanie na nowe zagrożenia. W przypadku BEAST, wykrywanie opiera się na bardzo specyficznych kombinacjach złośliwych działań. W związku z tym łatwiej jest dodawać nowe reguły, będąc przy tym mniej podatnym na fałszywe alarmy.

Również możliwość retrospektywnego porównania IOC i retrospektywne usuwanie jest możliwe tylko w przypadku BEAST.

Dlaczego potrzebujemy BEAST, skoro mamy DeepRay?

Siła DeepRay polega na tym, że jest w stanie przejrzeć kamuflaż wirusa, co pozwala nam zidentyfikować rdzeń złośliwego oprogramowania. Początkowa identyfikacja rdzeni jest procesem ręcznym. W przypadku najbardziej powszechnych rodzin oprogramowania typu crimeware jest to zadanie do wykonania.

BEAST pomaga wypełnić lukę czasową pomiędzy analizą nowego rdzenia wirusa i reakcją modułu DeepRay. Ale poza najbardziej powszechnymi rodzinami oprogramowania crimeware, istnieje również duża liczba tych, które choć pojedynczo występują rzadko, sumarycznie odpowiadają za ogromną liczbę infekcji. Jeżeli powodem małej popularności jest to, że są to rodziny zagrożeń wykorzystywane w ukierunkowanych atakach, nie czyni ich to mniej niebezpiecznymi. Ponieważ BEAST nie polega na identyfikacji konkretnego rdzenia złośliwego oprogramowania, ale na ogólnej obserwacji złośliwego zachowania, BEAST pomaga zwalczać te zagrożenia dodając przy tym kolejną warstwę ochrony.