Inspektor Procesów
Dane Techniczne

Multi-Stage Detection Techniques: 1. Machine Learning 2. Hyper Detect 3. Sandbox Analyzer 4. Memory Protection 5. Process Inspector

Przegląd

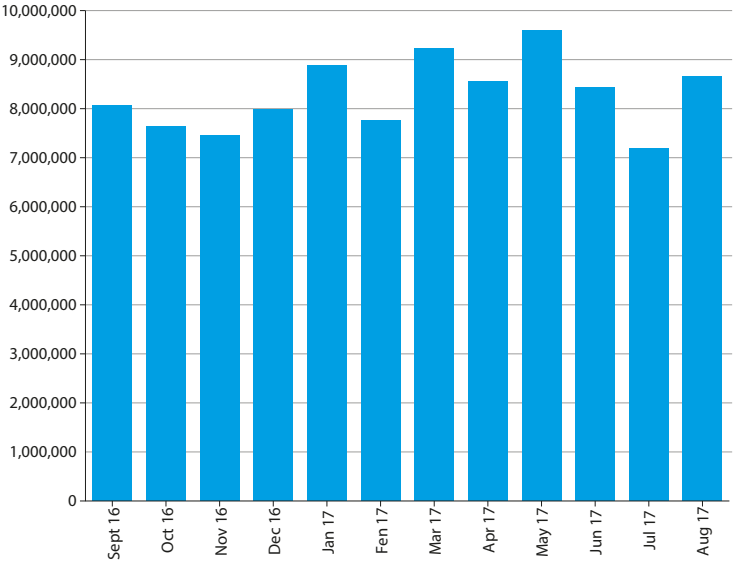
W obecnym krajobrazie cyberbezpieczeństwa, przedsiębiorstwa są stale narażone na działanie złośliwego oprogramowania, zakłócenia, naruszenia bezpieczeństwa danych oraz szereg innych incydentów wpływających na poprawne funkcjonowanie firmy. Platforma Bitdefender GravityZone Endpoint Security chroni punkty końcowe przed pełnym zakresem wyrafinowanych ataków cybernetycznych, zapewniając wysoką efektywność, niski wpływ na użytkowników końcowych i niskie koszty administracyjne. Składa się z wielowarstwowej ochrony, która stanowi dla hakerów nie lada wyzwanie. Każda z warstw ma na celu zablokowanie określonych typów zagrożeń, narzędzi lub technik ataków.

Inspektor Procesów Bitdefender jest częścią platformy GravityZone Endpoint Security. Jest to technologia wykrywania anomalii zachowania, która zapewnia ochronę przed nieoczekiwanymi zagrożeniami na etapie wykonywania.

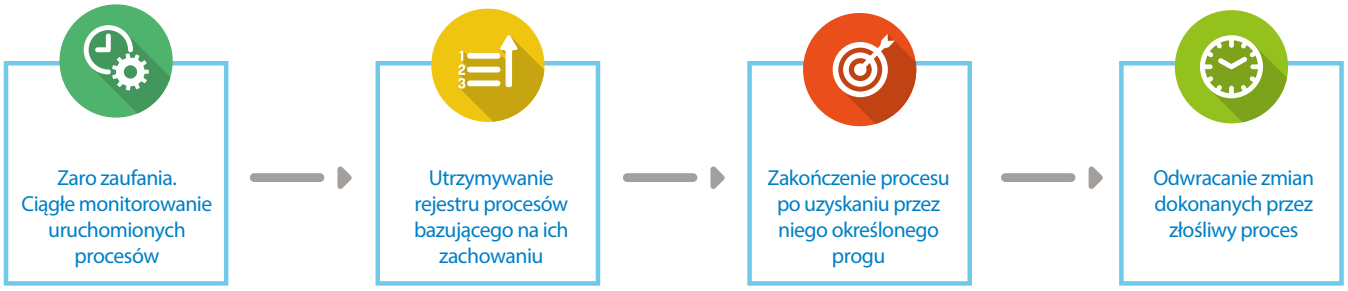
Etap Wykrywania	Typ Technologii	Zasięg Zagrożenia
Na Etapie Wykonania	Wykrywanie Anomalii w Zachowaniu	Zaciemnione złośliwe oprogramowanie, Ataki Ukierunkowane, Ataki oparte na Skryptach, Exploity, Opóźnione złośliwe oprogramowanie, Memory Attacks, Iniekcja Procesów, Eskalacja Uprawnień, Ataki file-less (np. Niewłaściwe użycie programu PowerShell), Ransomware

Znaczenie technologii Inspektora Procesów Bitdefender

Każdego dnia odkrywanych jest ponad 390 000 nowych złośliwych programów, dlatego ochrona twojego środowiska przed pojawiającymi się zagrożeniami oraz zagrożeniami zero-day staje się dla dzisiejszych zespołów bezpieczeństwa normą. Inspektor Procesów jest warstwą ochrony, która rozszerza kompleksowe technologie wykrywania przed wykonaniem na platformie GravityZone Endpoint Security. Radykalnie zmniejsza ryzyko uszkodzenia systemu przez nowe i pojawiające się zagrożenia. Działa na modelu "zero zaufania" i monitoruje procesy działające w systemie operacyjnym przy użyciu filtrów w trybie użytkownika i modelu jądra. Wyszukuje zachowanie specyficzne dla złośliwego oprogramowania
i przypisuje ocenę dla każdego procesu na podstawie jego działania i kontekstu. Jest to ważne, ponieważ każdy proces indywidualnie może nie wskazywać na złośliwe intencje, ale zbiorowa analiza zapewnia lepszy wgląd. Gdy ogólny wynik procesu osiąga określony próg, proces ten jest zgłaszany jako szkodliwy i podejmowane są odpowiednie działania naprawcze, w tym wycofywanie zmian wprowadzonych przez złośliwy proces w punkcie końcowym.



Last update: 09-05-2017 8:29



Funkcje

- **Śledzenie anomalii w zachowaniu**: Aktywne aplikacje i procesy są na bieżąco monitorowane. Przykłady: kopiowanie lub przenoszenie plików w folderach Systemu, folderach systemu Windows lub lokalizacjach dysku z ograniczonym dostępem, wykonywanie lub wprowadzanie kodu w przestrzeni innego procesu w celu uruchamiania z wyższymi uprawnieniami, uruchamianie plików, które zostały utworzone z informacjami przechowywanymi w pliku binarnym, autoplikacja, tworzenie wpisu automatycznego uruchamiania w rejestrze, uzyskiwanie dostępu lub wykonywanie nielegalnych operacji w lokalizacjach rejestru wymagających podwyższonych uprawnień, upuszczanie i rejestrowanie sterowników, niewłaściwe użycie PowerShell - np. sprawdź, czy uruchamiana jest funkcja powershell.exe z kilkoma określonymi argumentami wykrywanie określonego ransomware - np. usuwanie plików zapasowych / kopii shadow, generowanie kluczy szyfrowania i więcej
- **Automatyczne Działanie**: Automatycznie ocenia działające procesy i działa po wykryciu zagrożenia
- **Rollback/clean up**: Utrzymuje ścieżkę audytu zmian wprowadzonych przez proces na punkcie końcowym. Po wykryciu zagrożenia automatycznie zatrzymuje proces i wycofuje złośliwe zmiany przez niego wprowadzone.
- **Wykluczenie Procesu**: Możliwość wyłączenia procesów z monitorowania
- **Sprzężenie zwrotne z Bitdefender Global Protective Network (GPN)**: Zagrożenia wykryte przez Inspektora Procesu są natychmiast zgłaszane do chmury bezpieczeństwa Bitdefender, Globalnej Sieci Ochronnej Bitdefender (GPN), aprawiając, że nawet systemy po drugiej stronie kuli ziemskiej będą w stanie wykryć zagrożenie.

Korzyści

- Wykrywa zaawansowane ataki wcześniej i zapobiega naruszeniom, zmniejszaj koszty i wysiłki związane z reagowaniem na incydenty
- Inspektor Procesów znacznie zwiększa wskaźnik wykrywalności złośliwych programów, w tym ataków file-less, poprzez monitorowanie procesu przez cały okres jego istnienia i polegając na rzeczywistych charakterystykach zachowania, zamiast na sygnaturach, kodach binarnych czy podpisach cyfrowych
- Ochrona przed zaciemnionym złośliwym oprogramowaniem, atakami celowanymi, atakami niestandardowymi, atakami na pamięć, iniekcją procesu, eskalacją uprawnień, atakami file-less (np. Niewłaściwym użyciem programu PowerShell), ransomware
- Automatyczne cofanie szkodliwych zmian w systemie zapewnia zespołom ds.Bezpieczeństwa spokój
- Jest gotowy do użytku i nie wymaga włączania ani pisania złożonych reguł
- Inteligentna optymalizacja wydajności dla monitorowania aplikacji i procesów zapewnia niski wpływ na system
- Informacje zebrane z detekcji Inspektora Procesów są wykorzystywane do ulepszania modeli uczenia maszynowego odpowiedzialnych za wykrywanie na etapie przed wykonaniem
- Jest częścią jednego, zintegrowanego agenta bezpieczeństwa punktów końcowych i platformy centralnego zarządza nia, co redukuje obciążenia administracyjne
- Klienci nie muszą wdrażać kilku rozwiązań bezpieczeństwa punktów końcowych

Bitdefender

Bitdefender jest światowym dostawcą zabezpieczeń, który zapewnia najnowocześniejsze kompleksowe rozwiązania bezpieczeństwa ponad 500 milionom użytkowników w ponad 150 krajach. Bitdefender od 2001 roku tworzy nagradzane technologie zabezpieczeń dla firm i konsumentów oraz dostarcza rozwiązania z zakresu bezpieczeństwa infrastruktury hybrydowej i ochrony punktów końcowych. Dzięki R&D, współpracy i partnerstwu, Bitdefender ma wiodącą pozycję na rynku, zapewniając niezawodne zabezpieczenia, na których można polegać. Więcej informacji znajduje się na stronie: http://www.bitdefender.com.

www.bitdefender.pl | www.marken.com.pl | Marken Systemy Antywirusowe | tel: 58 573 51 51 | ul. Jana Hieronima Derdowskiego 7, 81-369 Gdynia