MORPHISEC
Moving Target Defense

CYBER EXPERTS

MORPHISEC SKUTECZNIE UODPARNIA KOMPUTERY

Chroń swoją firmę przed zagrożeniami typu zero-day i zaawansowanymi atakami, których celem są twoje niezałatane luki. Technologia obrony ruchomego celu Morphisec maskuje twoje aplikacje i przeglądarki internetowe i wychwytuje wszelkie próby dostępu. Twoje punkty końcowe, niegdyś słabe punkty, stają się nieprzeniknioną linią obrony.

LUKI W SYSTEMIE BEZPIECZEŃSTWA

Napastnicy są bardziej wyrafinowani, kreatywni i uparci niż kiedykolwiek, co roku wypuszczają miliony złośliwych odmian zagrożeń. Wykorzystują swą głęboką wiedzę o środowisku docelowym, aby rozwijać podstępne, wysoce ukierunkowane ataki - zwłaszcza typu Advanced Persistent Threats (APT) i zero-day, w tym samym czasie czerpiąc korzyści z niezałatanych luk.

Aby zwiększyć skalę zniszczeń, atakujący używają polimorfizmu, zaciemniania, szyfrowania i innych zaawansowanych technik, w celu obejścia mechanizmów zabezpieczeń i uniknięcia wykrycia. Zgodnie z tradycyjnym paradygmatem Detection & Remediation - nawet przy skomplikowanych rozwiązaniach behawioralno - analitycznych - aplikacje pozostają narażone od momentu pojawienia się nowego ataku, do chwili gdy zostanie publicznie ujawniony, zostanie opracowane rozwiązanie i wdrożenie łatki.

ROZWIĄZANIA TRADYCYJNE I "NEXT-GENERATION"

Rozwiązania ochrony w punkcie końcowym zazwyczaj wykorzystują jedno lub kombinację poniższych:

- Narzędzia, które wymagają znajomości sygnatury ataku, zrozumienia zachowań lub schematu ataku, takie jak: antywirusy, bramy sieciowe i systemy HIPS. Takie systemy są łatwo omijane przez ataki typu zero-day lub polimorficzne.
- Antywirusy nowej generacji, wykorzystujące analizę statyczną i sztuczną inteligencję czy zdolności uczenia się. Opierają się one na znanych schematach ataku i potrafią wykrywać znane ataki, ale nie typu zero-day.
- Kontrola aplikacji oraz podobne narzędzia, które wymagają znacznego wysiłku przy konfiguracji. Skonfigurowane zbyt ciasno mogą powodować fałszywe alarmy i wpływać na wydajność, a zbyt luźno - pozwalają pracownikom na swobodne wykonywanie pracy, ale ataki mogą przejść niezauważone.
- Rozwiązania typu containment, takie jak sandboksy. Mogą to być rozwiązania robocze do aplikacji, które nie wymagają natychmiastowego połączenia z siecią wewnętrzną, ale są łatwo omijane przez atakujących rozpoznających środowisko sandboxu.
- Narzędzia typu detection and remediation. Często skuteczne w wykrywaniu ataków, ale wymagają intensywnej analizy w celu odróżnienia faktycznych ataków od licznych fałszywie alarmów, co pochłania czas spółki, zasoby i osłabia efektywność biznesu.

MORPHISEC
Moving Target Defense

CYBER EXPERTS

MORPHISEC - RADYKALNIE ODMIENNE PODEJŚCIE

Zapobiegając zagrożeniom w punktach końcowych, Morphisec chroni twoje punkty końcowe przed wszelkimi atakami opartymi na złośliwym kodzie, atakami typu memory injection w końcowych aplikacjach, takich jak przeglądarki i inne narzędzia. Zapobiega atakom typu evasive, zero-day i atakom skierowanych w znane, ale niezałatane luki. Czyni to w sposób deterministyczny, bez fałszywych alarmów, poprzez nieobciążającą system usługę 1MB, nie wymagającą administracji.

Morphisec zmienia paradygmat zabezpieczeń na proaktywną, wczesną profilaktykę, która wykorzystuje taktykę hakerów, aby pokonać ich własną bronią. Technika obrony ruchomego celu zmienia środowisko uruchomieniowe, tak że autoryzowany kod działa bezpiecznie, podczas gdy złośliwy kod jest blokowany. Dzięki zapobieganiu atakom, zanim w ogóle dojdzie do skutku, Morphisec zmienia ekonomikę bezpieczeństwa, obcinając koszty i minimalizując zakłócenia i szkody dla biznesu.

Jak to działa:

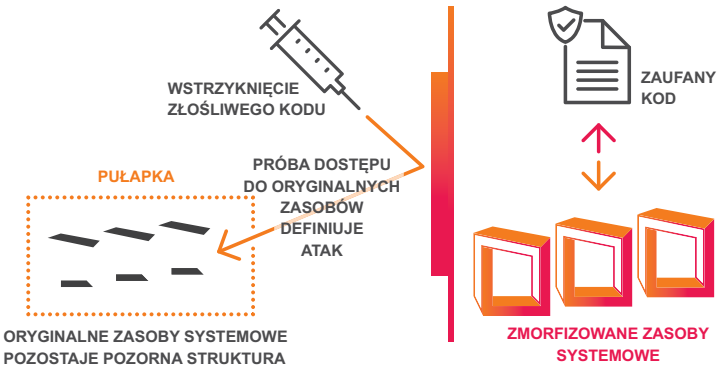
1. Gdy aplikacja ładuje się do miejsca w pamięci, silnik polimorficzny zmienia wewnętrzną strukturę procesu,jego wywołania do bibliotek i adresy bibliotek. Każdy przebieg jest unikatowy, dla procesu i dla instancji procesu. Sprawia to, że pamięć jest nieprzewidywalna dla atakujących.

2. Aplikacja działa normalnie z przekształconą strukturą, podczas gdy Morphisec utrzymuje atrapę oryginału do wykorzystania jako pułapkę.

3. Złośliwy kod nie zostanie wykonany i nie może uzyskać dostępu do żadnej z funkcji, których potrzebuje, ponieważ łańcuch destrukcji jest zatrzymywany na samym jego początku. Ataki nadal celują w oryginalną strukturę, nie wiedząc, że jest to jedynie atrapa.

4. Ataki na ten obszar pamięci są z definicji złośliwe, zostają zablokowane w pułapce. Ataki są rejestrowane i zgłaszane do Panelu Zarządzania Morphisec lub SIEM organizacj., Obszerne dane dotyczące ataków i zrzuty pamięci mogą być wysyłane do innych systemów.

Wewnątrz Obszaru Pamięci:



ZALETY W SKRÓCIE

NEUTRALIZOWANIE ZAAWANSOWANYCH ZAGROŻEŃ: Zapobiega wszelkim zagrożeniom typu zero-day i zaawansowanym atakom, nie wymagając żadnej wcześniejszej wiedzy o postaci, rodzaju i zachowaniu się zagrożenia.

ZAMYKANIE LUK: Stałe zarządzanie łatkami bezpieczeństwa wymaga czasu, pieniędzy i zasobów, a opóźnienia zwiększają ryzyko. Morphisec zabezpiecza luki w punktach końcowych.

BEZPROBLEMOWO: Instalacja bez ponownego uruchamiania i bez potrzeby konserwacji.Bez baz danych, podpisów lub aktualizacji zasad, bez analizy logów i alertów.

BEZ ZAKŁÓCEŃ W WYDAJNOŚCI: Niezwykle lekka usługa, aktywna tylko w czasie ładowania, minimalne rozmiary, bez zakłóceń wydajności i bez fałszywych alarmów.

AUTONOMIA: Chroni urządzenia pracowników wewnątrz i na zewnątrz sieci firmowej.

OCHRONA W CZASIE RZECZYWISTYM: Blokuje i więzi ataki zanim wyrządzą szkody. Ochrona nie zależy od połączenia z serwerem.

ZMIANA EKONOMIKI ATAKU: Zmienia zasady gry, tak że atakujący musi teraz ścigać cel. Eliminuje koszty związane z polowaniem na ataki, badaniem tzw. false positives i naprawą uszkodzeń.

ARCHITEKTURA ROZWIĄZANIA

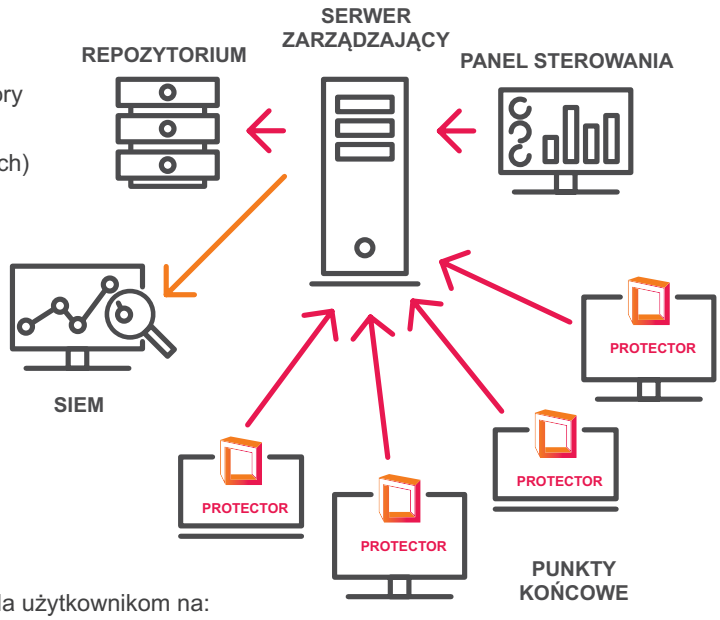
w punktach końcowych Morphisec wykorzystuje wielowarstwową architekturę klasy korporacyjnej, która jest wysoce skalowalna w zakresie danych i punktów końcowych. Jej elementy składają się z:

Ochrona Punktów Końcowych

Centralna część, Protector, działa autonomicznie na komputerach wyposażonych w Windows i serwerach opartych na Windows, fizycznych lub wirtualnych, a także bezpiecznie łączy się z serwerem zarządzania znajdującym się lokalnie lub w chmurze, dla celów sprawozdawczych. Protector jest wstępnie skonfigurowany i natychmiast chroni powszechnie atakowane aplikacje - takie jak programy MS Office i przeglądarki internetowe - z opcją łatwego dodania dowolnej innej aplikacji.

Serwer Zarządzający

Składnik ten, to wysoce skalowalny zestaw usług, który może obsługiwać organizację o dowolnej wielkości (od kilku do kilkudziesięciu tysięcy punktów końcowych) w jednym lub wielu miejscach konfiguracji. Obsługuje złożone i heterogeniczne środowiska IT, ze strukturą opracowaną tak, aby zapewnić odporność na uszkodzenia, zapewniając jednocześnie wysoką dostępność. Serwer zarządzania, dostarczany jako znajdujący się lokalnie lub w chmurze, obsługuje zarządzanie i śledzenie wszystkich Protectorów, integrację z SIEM i panel sterowania.



Panel Sterowania

Przejrzysty i konfigurowalny panel sterowania pozwala użytkownikom na:

Zarządzanie Protectorami

- zarządzanie punktami końcowymi,
- definiowanie polityki i przypisywanie je do grup,
- sprawdzanie stanu Protectora,

Wgląd do informacji o ataku

- wgląd w czasie rzeczywistym w ataki,
- szybkie przeglądanie aktualnego stan ataków na organizację,
- dodatkowe uwagi do przeprowadzania analiz,
- korelacje ataków z innymi atakami na organizację,
- łatwe filtrowanie, sortowanie i raportowanie informacji

Odpowiednie dla dużych przedsiębiorstw oraz małych i średnich firm

Morphisec dostosowuje się do indywidualnych potrzeb biznesowych zarówno dużych, jak i mniejszych organizacji, bez zakłócania działalności. Rozwiązanie płynnie łączy się z systemami bezpieczeństwa SIEM w większych korporacjach. Jednak nie jest konieczna codzienna konserwacja lub ustawianie zasad, a przechwycone dane nie są niezbędne do działania rozwiązania. Zatem małe i średnie firmy z ograniczonymi zasobami uzyskują taki sam poziom ochrony, jak duże przedsiębiorstwa. A ponieważ Morphisec ma zerowy wpływ na wydajność w czasie operacji, łatwo obsługuje punkty końcowe, które wymagają wysokiej wydajności.

Solidna Samoobrona

Rozbudowane aplikacje zabezpieczające są coraz bardziej popularnym celem ataku dla malware. Rozbudowana samoobrona Morphisec obejmuje funkcje sabotażowe Protectora, zweryfikowane serwery i szyfrowaną komunikację, które używają zastrzeżonych najnowocześniejszych technologii.

WYMAGANIA TECHNICZNE

Ochrona Punktów Końcowych	Zarządzanie Serwerem
wymagania sprzętowe	
sprzęt rekomendowany przez Microsoft do uruchomienia programu	■ intel 64-bit Pentium 2 CPU 8 core hyper-threading, rekomendowany RAM 8Gb, minmalnie 4Gb. ■ wielkość dysku: rekomendowana 1T, minimalna 250 Gb ■ dysk rekomendowany: raid 5 z backupem. Minimalny: raid 0
wymagania programowe	
■ Microsoft Windows 7 (32-bit and 64-bit) ■ Microsoft Windows 7, service Pack 1 (32-bit and 64-bit) ■ Microsoft Windows 8, 8.1 ■ Microsoft Windows 10 ■ Microsoft .net 4.5 lub wyższy	■ Windows server 2012 R2

O MORPHISEC

Morphisec jest tworzony przez czołowych ekspertów bezpieczeństwa z Izraela, zapewnia najwyższy poziom zapobiegania zagrożeniom dając pewność, upewniając się że atakujący nigdy nie znajdą poszukiwanych celów.

Morphisec zasadniczo zmienia scenę cyberbezpieczeństwa poprzez przesunięcie korzyści na rzecz obrońców, sprawiając, że dzięki technice obrony ruchomego celu są o krok przed atakującymi.

Więcej informacji na stronie internetowej www.cyberexperts.pl