THREAT PREVENTION

Kompleksowa ochrona sieci przed exploitami oraz szkodliwym oprogramowaniem

Firmy stoją przed koniecznością obrony przed różnego rodzaju zagrożeniami pochodzącymi z całego świata, przeprowadzanymi przez osoby, które chcą w ich wyniku odnieść korzyści finansowe. Ataki przeprowadzane dzisiaj znacznie różnią się od tych, które można było spotkać 15 lat temu. W celu uzyskania dostępu do wewnętrznej sieci wykorzystywane są różne techniki maskujące, od fałszowania pakietów oraz ich szyfrowania, po różnego rodzaju wieloetapowe dostarczanie kodu i korzystanie z technik fast-flux DNS, które pomagają jednocześnie pozostać niewidocznym dla tradycyjnych narzędzi ochronnych.

- Usługi zapobiegania zagrożeniom, wykorzystują nową generację rozwiązań zabezpieczających, stworzonych specjalnie z myślą o ochronie sieci przed szerokim spektrum zagrożeń.
- Pełne skanowanie ruchu sieciowego, zarówno w kontekście działań aplikacji, jak i użytkowników.
- Zapobieganie zagrożeniom na każdym etapie cyber-ataku
- Architektura wykorzystująca jednoprzebiegowe skanowanie pozwala na utrzymanie wysokiej wydajności działania, nawet w sytuacji, w której wykorzystywane są wszystkie funkcje zapobiegania zagrożeniom
- Pojedyncza tabela polityk bezpieczeństwa zmniejsza narzut czasu przeznaczony na zarządzanie
- Codzienne, automatyczne aktualizacje zabezpieczeń przed złośliwym oprogramowaniem lub wpisami DNS

Niestety w chwili obecnej rozwiązania zabezpieczeń sieci opierają się na strategiach ochrony powstałych przed ewolucją i pojawieniem się nowych metod ataku. Ruch sieciowy jest kontrolowany wyłącznie na niektórych portach, a dodawanie kolejnych jednofunkcyjnych urządzeń do potoku zabezpieczeń może doprowadzić do obniżenia wydajności oraz niskiej przejrzystości konfiguracji. Prowadzi to do niebezpiecznej sytuacji, kiedy w zabezpieczeniach powstają luki, spowodowane fragmentacją rozwiązań, a co za tym idzie utrudnienia w zarządzaniu, co - coraz sprytniejszym napastnikom - ułatwia penetrację sieci.

Palo Alto Networks® na nowo zdefiniowało zabezpieczenia sieci, stosując podejście zerowego zaufania. Umożliwiamy bezpieczne korzystanie z aplikacji, zapewniając ochronę przeciw zaawansowanym cyber-atakom w każdej ich fazie, stosując do tego celu wielofunkcyjną platformę dokonującą analizy całego ruchu sieciowego, na wszystkich portach i odnośnie wszystkich protokołów, przeprowadzaną w jednym, zbiorczym skanowaniu.

PKorzystaj z aplikacji, zapobiegaj zagrożeniom

Aplikacje są integralną częścią dzisiejszej rzeczywistości i z tego powodu stały się bardziej dostępne dla użytkowników, pozwalając na wejście do sieci za pomocą szyfrowanych kanałów komunikacji, korzystanie z niestandardowych portów lub przełączanie się między portami – wszystko w celu zagwarantowania im stałego dostępu.

Niestety zaawansowane zagrożenia wykorzystują w celu ukrycia swej działalności nowe drogi, którymi aplikacje są udostępniane użytkownikom. Stosowane są rozwiązania polegające na tunelowaniu swojego kodu w aplikacjach lub ukrywanie swojej obecności w ruchu szyfrowanymi połączeniami SSL – wszystko w celu ustanowienia swego rodzaju przyczółka w atakowanej sieci i rozpoczęcia z niego dalszej działalności.

Rozwiązania Palo Alto Networks® zapewniają ochronę przed tego rodzaju zagrożeniami, udostępniając wiele poziomów zapobiegania i zwalczania ataku w każdej jego fazie. Subskrypcja naszych rozwiązań obejmuje zapobieganie włamaniom, sieciowe zabezpieczenia przed szkodliwym oprogramowaniem, ochronę

przed działaniem programów do zdalnej kontroli zainfekowanych maszyn (command-and-control) oraz chroni przed innymi zaawansowanymi atakami poprzez identyfikowanie i skanowanie całego ruchu sieciowego – zarówno pod kątem aplikacji, użytkowników lub danych, obejmując swą kontrolą zarówno ruch szyfrowany, jak i nieszyfrowany odbywający się na wszystkich protokołach i na wszystkich portach.

Eliminacja zagrożeń przy każdej okazji

Niemal każde naruszenie bezpieczeństwa sieci w atakowanej organizacji odbywa się przez ominięcie pojedynczego mechanizmu ochrony. Palo Alto Networks® wprowadza zintegrowane technologie obronne wzajemnie wspierające się w wychwytywaniu zagrożeń – jeżeli atak ominął jedną blokadę, zostaje powstrzymany przez inną. Kluczem do skutecznej ochrony jest korzystanie z zabezpieczeń zorientowanych na cel oraz korzystających z mechanizmów wymiany informacji i budowy kontekstu, zarówno wokół zdarzeń związanych z kontrolowaną przez nie transmisją, jak i identyfikacją oraz blokowaniem zagrożeń.

Rekomendacja zabezpieczeń

Palo Alto Networks® jest jedynym dostawcą rozwiązań, który osiągnął 100-procentowy wskaźnik blokady exploitów w teście 2015 Next Generation Intrusion Preventing System (NGIPS) przeprowadzanym przez NSS Labs.

Zapobieganie włamaniom

Ochrona przed zagrożeniami wykrywa i blokuje próby włamań stosujące – zarówno w warstwie sieciowej, jak i warstwie aplikacji – techniki ukrywania działalności takie, jak skanowanie portów, przepełnienie bufora, zdalne wykonywanie kodu, fragmentację protokołu lub maskowanie. Wykonywane jest to na podstawie porównania zgodności sygnatur i wykrywania anomalii, którym objęte jest sprawdzanie i analiza protokołów, a następnie korzystanie z technik uczenia się do przekazywania ostrzeżeń i blokowania ruchu odbywającego się według rozpoznanych, szkodliwych wzorców. Wykrywanie ataków odbywa się na podstawie sprawdzania zgodności wzorców na wielu pakietach danych, włącznie ze sprawdzaniem kolejki ich przesyłania, co daje możliwość dopuszczenia wyłącznie pożądanego ruchu, w którym nie wykryto technik ukrywania złośliwego kodu.

- Analiza oparta na sprawdzaniu protokołów w pierwszej kolejności dokonuje dekodowania ruchu, a następnie aplikacji sygnatur celem wykrycia exploitów działających zarówno w warstwie sieciowej, jak i warstwie aplikacji.
- Ponieważ istnieje wiele sposobów wykorzystania danej luki bezpieczeństwa, stosowane przez nas sygnatury zapobiegania włamaniom zbudowane są w oparciu o nią samą, co pozwala na większą dokładność w powstrzymywaniu ataków ze strony różnych exploitów. Stosując pojedynczą sygnaturę możliwe jest powstrzymanie wielokrotnych prób wykorzystania znanej luki w bezpieczeństwie sieci lub aplikacji.
- Ochrona oparta na wykrywaniu anomalii dla danego protokołu dokonuje analizy zgodności ruchu z opublikowanymi dokumentami RFC i blokuje zbyt długie adresy stron internetowych lub próby logowania do serwerów FTP.
- Analiza heurystyczna sprawdza wzorce ruchu i wykrywa anomalie takie, jak skanowanie portów, wykrywanie hostów, ataki DoS oraz tzw. flood.
- Inne funkcje obejmują m.in. blokowanie nieprawidłowych lub zniekształconych pakietów danych, defragmentację pakietów, ponowne zestawianie połączeń TCP, co również pozwala na ochronę przed technikami maskowania i ukrywania ataku.
- Łatwe do skonfigurowania, niestandardowe, tworzone przez użytkownika sygnatury pozwalają na dopasowanie narzędzi zabezpieczających do specyficznych potrzeb danej sieci

Oprócz tradycyjnych funkcji zapobiegania włamaniom, rozwiązania Palo Alto Networks® zapewniają wyjątkowe możliwości wykrywania i blokowania zagrożeń wykorzystujących dowolny port w miejsce rozwiązań korzystających z baz sygnatur przypisanych do konkretnej listy zdefiniowanych portów. Nowa generacja firewall przypisuje aplikacjom oddzielne identyfikatory, które pozwalają na kontrolę całości ruchu na wszystkich portach, gdyż mechanizmy zabezpieczające nigdy nie tracą ze swojego pola widzenia podejrzanego ruchu.

Ochrona przed złośliwym oprogramowaniem

Wbudowana ochrona przed złośliwym oprogramowaniem pozwala powstrzymać ataki zanim dotrą one do docelowego hosta, korzystając z sygnatur bazujących na przekazywanych danych, a nie zakodowanym ich skrócie (hash). Rozwiązania Palo Alto Networks® blokują działanie szkodliwego oprogramowania obejmując również jeszcze nie spotykane warianty. Strumieniowy silnik skanowania chroni sieć bez wprowadzania niepożądanych opóźnień, co jest poważnym problemem opro-

SYGNATURY BAZUJĄCE NA TREŚCI WOBEC SYGNATUR BAZUJĄCYCH NA HASHACH

Skanowanie zawartości oparte na sygnaturach może wykrywać wzorce, które określają przeznaczenie pliku.

Sygnatury oparte o hashe dokonują wykrywania i porównań bazując na kodowaniu pliku. Hashe plików są proste do zmiany, dlatego też oparte na nich wykrywanie nie jest skuteczne w przypadku złośliwego oprogramowania opartego o polimorficzny kod lub różne warianty tego samego pliku.

Korzystanie z sygnatur opartych o hashe można porównać do określania zawartości pudełka tylko poprzez spojrzenie na jego wygląd, bez sprawdzenia jego zawartości.

gramowania antywirusowego opartego na serwerach proxy. Ochrona przed szkodliwym oprogramowaniem z Palo Alto Networks® dokonuje inspekcji ruchu w momencie otrzymania pierwszego pakietu danych pliku, eliminując zarówno zagrożenia, jak też problemy związane z wydajnością występujące w tradycyjnych rozwiązaniach stand-alone. Podstawowe funkcje ochrony obejmują:

- Strumieniowe wykrywanie i ochronę przed złośliwym oprogramowaniem ukrytym wewnątrz skompresowanych plików lub zawartości z sieci Web.
- Ochrona przed kodem ukrytym wewnątrz znanych typów plików, jak dokumenty pakietu Microsoft® Office® lub pliki PDF.
- Aktualizacje WildFire™ zapewniające ochronę przed najnowszymi odmianami szkodliwego kodu.

Sygnatury dla wszystkich typów złośliwego oprogramowania są generowane bezpośrednio na podstawie milionów próbek zebranych przez Palo Alto Networks®, w tym dotychczas nieznanych próbek przesłanych do Wildfire, globalną sieć pułapek i inne wiodące organizacje badawcze firm trzecich z całego świata.

Ochrona przed działaniem złośliwych programów do zdalnej kontroli

Zdajemy sobie sprawę, że nie istnieje skuteczne panaceum pozwalające na zapobieganie przedostaniu się do sieci wszystkich możliwych zagrożeń. Po początkowej infekcji atakujący przejmuje zdalną kontrolę nad hostem i tworzy kanał do pobierania dalszych porcji złośliwego kodu, którego uruchomienie pozwala wykonywać kolejne instrukcje lub dokonać kradzieży danych.

Oferowane przez nas narzędzia do ochrony odcinają żądania ruchu wychodzącego do znanych domen ze szkodliwym oprogramowaniem oraz ze znanych narzędzi zainstalowanych na zainfekowanych urządzeniach.

Przechwytywanie i kontrola ruchu do serwerów DNS

Oferowana przez nas ochrona idzie o krok dalej, udostępniając narzędzia typu sinkholing do przechwytywania i blokady połączeń ze złośliwymi serwerami DNS, zapobiegając eksfiltracji i pozwalając na precyzyjną identyfikację ofiary. Konfiguracja serwera przechwytującego pozwala na przekierowanie każdego ruchu wychodzącego do szkodliwej domeny lub adresu IP, do wybranego adresu IP w wewnętrznej sieci. Pozwala to na efektywną blokadę połączeń złośliwego oprogramowania do zdalnej kontroli, powstrzymując ruch wychodzący niezależnie od częstotliwości czy pory dnia, w których wykonywane są próby jego nawiązania oraz tworzenie raportu hostów wewnątrz sieci, próbujących nawiązać takie połączenia. Zespoły do reagowania na zagrożenia codziennie dostają listy zaatakowanych maszyn, którymi muszą się zająć, jednocześnie mogąc pracować bez stresu, ponieważ komunikacja z atakującym została odcięta.

WildFire™

Informacje o wykrywanych każdego dnia domenach ze szkodliwym oprogramowaniem są dostarczane do bibliotek zabezpieczeń poprzez WildFire™, wdrożonym przez nas wirtualnym środowiskiem do analizy złośliwego kodu, co pozwala na utrzymywanie aktualności ochrony przed najnowszymi zagrożeniami na każdym etapie ataku.

Zautomatyzowana korelacja obiektów

Rozwiązania Palo Alto Networks® obejmują zdolność do identyfikacji obecności zaawansowanych zagrożeń poprzez monitorowanie i korelację ruchu sieciowego oraz dzienników zagrożeń, dzięki czemu można szybko zidentyfikować zainfekowanych użytkowników i dokonać analizy dziwnych wzorców zachowań. Korelacja obiektów obejmuje badanie i analizę nieznanych zagrożeń w tzw. Unit 42 ze środowiska Wildfire™, co w połączeniu z identyfikatorem użytkownika (User-ID™) pozwala na korelację anomalii ruchu i wskaźników zagrożenia tak, by szybko i dokładnie zidentyfikować zainfekowane urządzenie w sieci. Nieznane lub anormalne pakiety TCP i UDP oraz wiele potencjalnie podejrzanych zachowań takich, jak powtarzające się pobierania, użycie dynamicznych serwerów DNS, próby wykorzystania exploitów i inne kluczowe zachowania są śledzone, a następnie kompilowane do postaci alertów zawierających zarówno listę zaatakowanych użytkowników, jak i listę czynników, które doprowadziły do postawienia takiej diagnozy.

Pełna przejrzystość i ograniczenie ryzyka

DOdszyfrowanie ruchu kanałów SSL

Blisko 40 procent ruchu sieciowego przeprowadzana jest przez szyfrowane kanały SSL, co może wygenerować dużą lukę w zabezpieczeniach sieci, jeżeli ruch nie zostanie odszyfrowany i przeskanowany pod kątem zagrożeń. Oferowana przez nas platforma ma wbudowane narzędzia pozwalające na selektywne deszyfrowanie przychodzącego lub wychodzącego ruchu przez kanały SSL. Po odszyfrowaniu, sprawdzeniu i potwierdzeniu bezpieczeństwa następuje ponowne szyfrowanie i zezwolenie na połączenie z punktem docelowym.

Blokowanie plików

Około 90 procent plików ze złośliwym kodem używanych podczas ataków typu phishing to pliki wykonywalne. W połączeniu z faktem, że 59 procent incydentów związanych z bezpieczeństwem jest wynikiem zaniedbań pracowników oznacza, że użytkownicy mogą nie dysponować wiedzą o tym co jest, a co nie jest bezpieczne. Redukowanie prawdopodobieństwa infekcji polega na zapobieganiu uzyskaniu dostępu do sieci plikom znanym z ukrywania złośliwego kodu, jak pliki wykonywalne. Funkcjonalność blokowania plików można połączyć z identyfikatorem użytkownika tak, by używać blokad dostępu bazując na zadaniach użytkowników, co pozwala zapewnić dostęp odpowiednim osobom do odpowiednich zasobów, jednocześnie zmniejszając ryzyko i spełniając zróżnicowane wymogi w danej organizacji. Dalsze zmniejszenie ilości możliwych ataków odbywa się przez zezwolenie wysyłania plików do środowiska WildFire™ w celu analizy i określenia, czy nie zawierają one nieznanego do tej pory złośliwego kodu.

Ochrona pobierania

Niczego nie podejrzewający użytkownicy mogą nieumyślnie pobrać złośliwe oprogramowanie po prostu odwiedzając ulubioną stronę w sieci Web. Bardzo często zarówno odwiedzający, jak i nawet właściciel danej witryny może nie zdawać sobie sprawy, że jej bezpieczeństwo zostało naruszone. Rozwiązania Palo Alto Networks® identyfikują potencjalnie niebezpieczne pobierania i wysyłają ostrzeżenie do

użytkownika w celu upewnienia się, że dane pobieranie jest zamierzone i zaaprobowane. Zapobieganie atakom z nowych i zmieniających się domen jest wykonywane przez powiązanie ich z politykami filtrowania adresów URL oraz blokowania plików.

Wykorzystanie globalnej sieci do zapobiegania atakom

Szczegółowe zestawienia ataków nie są przechowywane wyłącznie wewnątrz interfejsu zarządzania, lecz przekazywane do wszystkich mechanizmów ochronnych, w celu zapewnienia odpowiedniego kontekstu informacji. Do automatycznego wykrywania i dostarczania mechanizmów ochronnych wykorzystujemy dostępne globalnie środowisko WildFire™, co pozwala nam utrzymywać dla wszystkich klientów stały poziom bezpieczeństwa, również przed najnowszymi zagrożeniami.

Pasywne serwery DNS

Korzystanie z rozwiązań analizy zapytań do serwerów DNS pozwala na ochronę organizacji przed coraz szybciej ewoluującym szkodliwym oprogramowaniem i błyskawicznie pojawiającymi się niebezpiecznymi stronami www. Wdrożenie pasywnego monitorowania zapytań do serwerów DNS pozwala na zwiększenie poziomu ochrony poprzez sprawdzanie połączeń z globalnie tworzoną bazą złośliwych domen.

Światowej klasy laboratoria badawcze

Zespół badania zagrożeń Palo Alto Networks® jest organizacją badawczą światowej klasy, która wykrywa oraz dokonuje analizy zagrożeń, aplikacji oraz ich odpowiedniego zachowania w sieci. Zespół działa w celu zapewnienia bezpieczeństwa przed obszerną listą exploitów, badając za pomocą inżynierii wstecznej podatność na nowe zagrożenia. Każdego roku laboratoria badawcze Palo Alto Networks® odkrywają i raportują więcej błędów w produktach Microsoft, niż jakikolwiek inny dostawca rozwiązań zapewniających bezpieczeństwo.

Model	Przepustowość wykrywania
PA-200	50 Mbps
PA-500	100 Mbps
PA-2020	200 Mbps
PA-2050	500 Mbps
PA-3020	1 Gbps
PA-3050	2 Gbps
PA-3060	2 Gbps
PA-5020	2 Gbps
PA-5050	5 Gbps
PA-5060	10 Gbps
PA-7050	100 Gbps*
PA-7080	160 Gbps*

*włączony mechanizm DSRI

unit42

Palo Alto Networks® jest również miejscem pracy zespołu ekspertów Unit 42, którzy analizują dane zebrane przez globalną społeczność, w celu identyfikacji i badania nowych metod ataków, szkodliwego oprogramowania, aktywnych zagrożeń oraz przygotowywania raportów na temat najnowszych trendów.

Jednoprzebiegowe skanowanie pod kątem dowolnych zagrożeń

Rozwiązania zapobiegania zagrożeniom Palo Alto Networks® korzystają z jednoprzebiegowego silnika sprawdzającego i klasyfikującego ruch oraz wykrywającego i blokującego zarówno szkodliwe oprogramowanie, jak też podatność na exploity. Tradycyjne technologie zapobiegawcze wymagają użycia dwóch lub więcej silników skanujących, co skutkuje znacznymi opóźnieniami i dramatycznie obniża całkowitą wydajność. Rozwiązania Palo Alto Networks® wykorzystują zunifikowany format sygnatur dla wszystkich zagrożeń, co pozwala na wykonanie wszystkich analiz w jednym, zintegrowanym procesie skanowania, eliminując jednocześnie zbędne procesy wspólne dla rozwiązań wykorzystujących wiele silników skanujących.

Opracowana przez nas technologia zapobiegania zagrożeniom kontroluje każdy pakiet przechodzący przez platformę, sprawdzając sekwencje bajtów zarówno w nagłówku, jak i przesyłanych danych. Poprzez taką analizę jesteśmy w stanie dokonać identyfikacji ważnych informacji odnośnie pakietu, włączając w to aplikację do jego wysyłki, adres źródłowy i docelowy, zgodność protokołu ze specyfikacjami RFC oraz sprawdzenie, czy przesyłane dane zawierają kod exploita lub szkodliwego oprogramowania. Poza pojedynczymi pakietami analizujemy również kontekst zapewniony przez sprawdzenie kolejki przybycia i sekwencji wielu pakietów, co pozwala na wykrycie technik maskujących. Wszystkie te analizy oraz sprawdzanie zgodności z sygnaturami przeprowadzane są podczas pojedynczego skanowania, co pozwala na zachowanie potrzebnej przepustowości sieci.

paloalto NETWORKS®

4401 Great America ParkwaySanta Clara, CA 95054
Kontakt: +1.408.753.4000
Dział sprzedaży: +1.866.320.4788
Wsparcie techniczne: +1.866.898.9087
www.paloaltonetworks.com

PAN-DS-THREAT-PREVENTION-112515