WILDFIRE

WildFire: Ochrona przed ukierunkowanym i nieznanym szkodliwym oprogramowaniem

WildFire identyfikuje nieznany, złośliwy kod, exploity typu zero-day oraz zaawansowane zagrożenia poprzez dynamiczną analizę w skalowalnym, opartym o chmurę środowisku wirtualnym. WildFire automatycznie i niemal w czasie rzeczywistym rozsyła poprawki zabezpieczeń pozwalając zespołom odpowiedzialnym za bezpieczeństwo sieci sprostać wyzwaniom stawianym przez zaawansowane cyberataki. Zbudowana w oparciu o rozwiązania zabezpieczeń poziomu enterprise platforma klasyfikuje każdy rodzaj ruchu, włącznie z zagrożeniami oraz aplikacjami, które je powodują – niezależnie od portu, na którym przebiega komunikacja czy korzystanie z szyfrowania SSL.

- **Identyfikacja nieznanego złośliwego kodu oraz expliotów typu zero-day poprzez wykorzystanie zaawansowanych statycznych i dynamicznych metod analizy.**
- **Łączy pełną przejrzystość oraz kontrolę nad znanymi zagrożeniami i aplikacjami korzystając z dynamicznego sprawdzania nieznanych zagrożeń w chmurze w celu zapewnienia dokładnej, bezpiecznej i skalowalnej analizy szkodliwego kodu.**
- **Blokowanie w trybie in-line złośliwego kodu i zarażonych plików, jak również ruchu zdalnej kontroli (C2) nad zarażonymi stanowiskami.**

Zaawansowane techniki cyberataków wykorzystują metody ukrywania się w celu uniknięcia wykrycia przez tradycyjne rozwiązania zabezpieczające. Utalentowani przeciwnicy stawiają zespołom odpowiedzialnym za bezpieczeństwo wysokie wymagania, prowadząc do przewartościowania podstawowych założeń funkcjonowania systemów zapobiegających włamaniom, ochrony antywirusowej oraz narzędzi do uruchamiania kodu w środowiskach wirtualnych, pozwalających na pokonanie zaawansowanych zagrożeń.

Platforma bezpieczeństwa klasy enterprise

WildFire™ jest zbudowane w oparciu o najwyższej jakości platformę zabezpieczeń, zapewniającą pełen wgląd w ruch sieciowy, włącznie z podglądem aktywności mających na celu zapobieganie wykryciu niepożądanych działań, jak transmisja na niestandardowym porcie lub stosowanie szyfrowania SSL. Znane zagrożenia są aktywnie blokowane mechanizmem Threat Prevention, zapewniającym podstawową ochronę przed znanymi exploitami, złośliwym oprogramowaniem, przekierowaniem ruchu na strony www zawierające złośliwy kod lub programami wykonującymi kod umożliwiający zdalną kontrolę nad zaatakowanym komputerem (C2). WildFire przeprowadza analizę nieznanych plików w skalowalnym wirtualnym środowisku SandBox, które pozwala na identyfikację podejrzanych zachowań i uruchomienie mechanizmów ochronnych, automatycznie dostarczanych do użytkowników systemu. W rezultacie powstaje pętla pozwalająca na kontrolę cyberzagrożeń począwszy od identyfikacji i ograniczenia możliwości ataku, poprzez pełną kontrolę ruchu sieciowego na wszystkich portach i protokołach, automatyczne wykrywanie nieznanego kodu na podstawie zachowania w kontrolowanym środowisku wirtualnym, aż do automatycznej implementacji polityk bezpieczeństwa po wykryciu nowych metod ataków.

WildFire

WildFire to zaawansowane wirtualne środowisko do analizy złośliwego kodu, stworzone w celu wiernej emulacji rozwiązań sprzętowych oraz analizy podejrzanego kodu podczas jego uruchamiania. Usługa oparta jest o mechanizmy bazujące na rozwiązaniach chmurowych, wykrywających i blokujących

nieznany szkodliwy kod, exploity oraz wychodzące połączenia sieciowe do hostów typu Command and Control (C2), poprzez obserwację działań, zamiast poleganiu na wstępnie zdefiniowanych sygnaturach. Dodatkowo, informacje o dotychczas nierozpoznanych, zidentyfikowanych zagrożeniach są automatycznie rozsyłane do innych użytkowników, a czas propagacji nie przekracza 15 minut. Usługi zabezpieczeń oferowane przez Palo Alto Networks® obejmują m.in. nowej generacji firewalle, umożliwiające pełną kontrolę nad ruchem w sieci w sytuacji, w której cyberprzestępcy próbują dostarczyć złośliwy kod lub komunikować się z zarażonymi systemami.

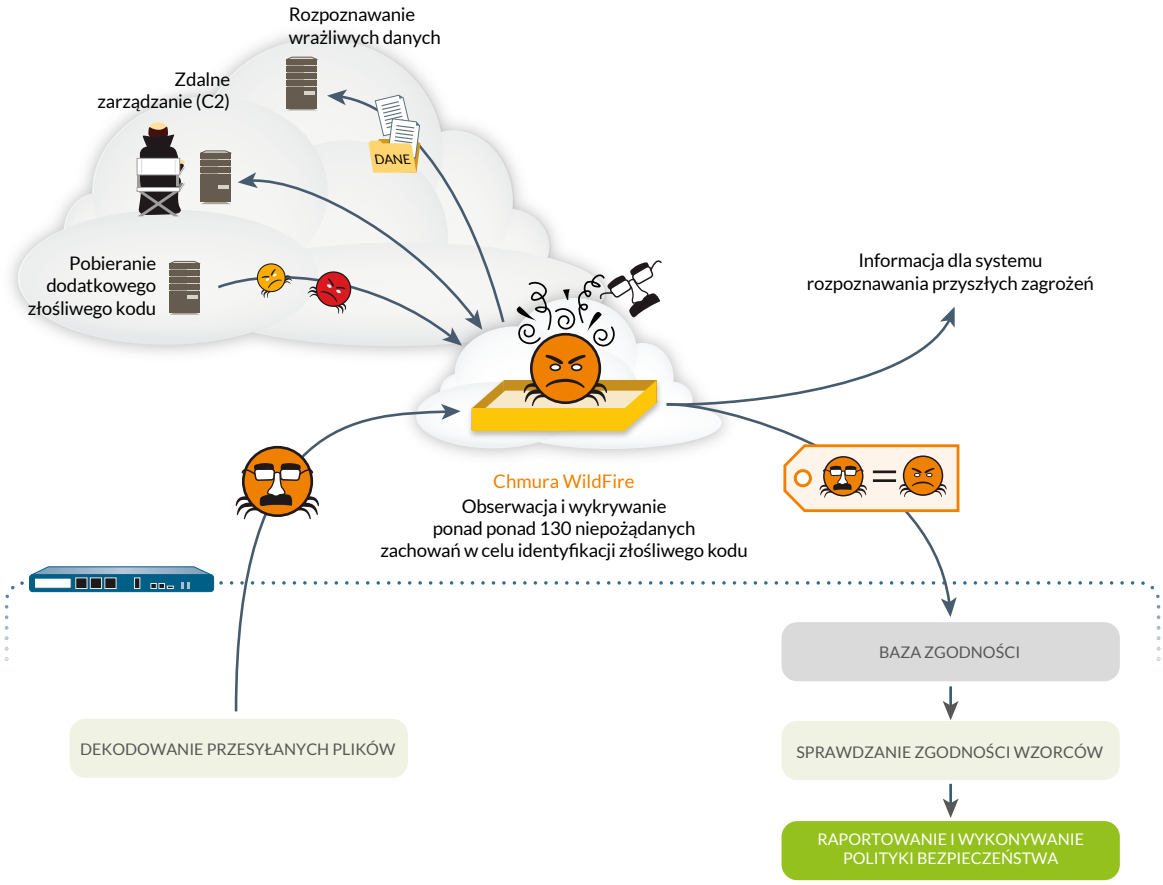
Wykrywanie zagrożeń oparte o analizę zachowań

W celu wykrycia nieznanego dotychczas złośliwego kodu lub exploitów, WildFire uruchamia podejrzaną zawartość w systemach Windows XP, Windows 7 lub Android dając jednocześnie pełen podgląd aktywności dla znanych typów plików, obejmujących: pliki wykonywalne (EXE), biblioteki (DLL), pliki skompresowane (archiwa ZIP), pliki PDF, dokumenty Office, wykonywalne pliki Java, aplikacje dla systemu Android, aplety Flash oraz strony internetowe z osadzonymi materiałami wysokiego ryzyka, jak skrypty w języku JavaScript, pliki Adobe Flash lub spreparowane pliki obrazów.

WildFire rozpoznaje ponad 200 zachowań potencjalnie generowanych przez złośliwe oprogramowanie, w celu identyfikacji plików zawierających złośliwy kod włącznie z:

- **Zmianami na komputerze hoście:** obserwacja wszystkich działających procesów i zmian dokonywanych na komputerze hoście, włącznie ze zmianami na plikach lub w rejestrze, wstrzykiwanie kodu, wykrywanie dokonywanych przez exploity zmian zawartości komórek pamięci, dopisywanie programów do automatycznego uruchamiania podczas startu systemu, dodawanie usług systemowych lub innych podejrzanych aktywności.
- **Podejrzanym ruchem sieciowym:** analiza aktywności sieciowej generowanej przez podejrzane pliki włączając w to mechanizmy otwierające backdoory, pobieranie szkodliwego kodu, odwiedziny domen o złej reputacji, skanowanie sieci i inne aktywności.
- **Wykrywaniem mechanizmów zapobiegających analizie:** monitoring technik wykorzystywanych przez zaawansowane szkodliwe oprogramowanie w celu uniknięcia analizy kodu w środowiskach wirtualnych takich jak: wykrywanie debuggowania kodu, wykrywanie systemu nadzorcy, wstrzykiwanie kodu w zaufane procesy, wyłączanie zabezpieczeń bazujących na regułach obowiązujących dla komputera hosta i inne.

Rozszerzenie platformy firewalla obejmuje natywną klasyfikację ruchu sieciowego sprawdzającą ruch z setek aplikacji, a WildFire oferuje unikalne testy zachowań niezależne od portów komunikacji lub stosowanego szyfrowania, dając pełen przegląd ruchu sieciowego włączając w to strony www, protokoły komunikacji dla poczty elektronicznej (SMTP, IMAP, POP) czy ruchu do serwerów FTP.



Jak działa WildFire: WildFire udostępnia kombinację nowej generacji sprzętowego firewalla oraz skalowalnej analizy złośliwego kodu, korzystając z rozwiązań opartych o chmurę

Architektura wykrywania zagrożeń oparta o rozwiązania chmurowe
W celu dynamicznej analizy zagrożeń sieciowych WildFire używa opartej o rozwiązania chmurowe architektury, pozwalającej na wykorzystanie dostarczanych przez Palo Alto rozwiązań typu firewall, które nie wymagają używania dodatkowego sprzętu. W sytuacji, w której przepisy nie pozwalają na korzystanie z publicznie dostępnej infrastruktury chmurowej, możliwe jest użycie prywatnej sieci opartej o urządzenia WF-500. W każdym innym przypadku WildFire zapewnia możliwość użycia najlepszych w swojej klasie, w pełni przezroczystych i efektywnych kosztowo rozwiązań.

Zapobieganie zagrożeniom dzięki globalnie dostępnym informacjom
W momencie wykrycia zagrożenia WildFire automatycznie generuje reguły zabezpieczeń, które stają się dostępne dla innych użytkowników w ciągu maksymalnie 15 minut. Tak szybkie dostarczanie aktualizacji informacji o zagrożeniach pozwala na identyfikację i powstrzymanie ich rozprzestrzeniania się bez konieczności wykonywania dodatkowej ich analizy. Klienci korzystający z globalnych rozwiązań Palo Alto Networks wzajemnie pomagają sobie w powstrzymywaniu ataków cyberprzestępców.

Dodatkowo ochrona zapewniana przez WildFire nie tylko zapobiega wykonywaniu złośliwego kodu lub użyciu plików zawierających taki kod, ale również blokuje niepożądaną komunikację wykonywaną przez oprogramowanie do zdalnej kontroli zarażonego komputera lub podmiany informacji odnośnie serwerów DNS. Informacje o niepożądanym działaniu są automatycznie wysyłane do systemu PAN-DB i jednocześnie blokowane są odkryte adresy stron internetowych zawierających złośliwy kod. Korelacja tak zebranych danych oraz działających jednocześnie mechanizmów ochronnych, pozwalają na identyfikację i zablokowanie zarówno aktualnie dostępnych metod ataku, jak i potencjalnych, przyszłych zagrożeń.

Zintegrowane logowanie, raportowanie oraz analiza śledcza
Użytkownicy rozwiązań WildFire otrzymują zestaw zintegrowanych informacji, obejmujących logi zdarzeń, ich analizę oraz dostęp do interfejsu zarządzania, dzięki czemu osoby odpowiedzialne za bezpieczeństwo sieci mogą w szybki sposób skorzystać z mechanizmów portalu WildFire lub narzędzia Panorama, w celu sprawdzenia i korelacji zdarzeń mających miejsce w ich sieci. Pozwala to personelowi na szybką lokalizację zdarzeń wymagających reakcji. Znakowanie hostów lub sieci, które uległy atakowi pozwala na podjęcie natychmiastowych działań w oparciu o zapisy w logach oraz sygnatury stworzone przez użytkowników.

WildFire udostępnia ponadto personelowi takie narzędzia, jak:

- Szczegółowa analiza każdego podejrzanego pliku przesłanego do WildFire, z podziałem na systemy operacyjne, włącznie ze sprawdzeniem aktywności dla hosta lub sieci
- Dane sesyjne powiązane z procesem dostarczenia szkodliwego kodu, zawierające adresy źródła, cel, użytą aplikację, identyfikator użytkownika, docelowy adres URL, itp.
- Dostęp do oryginalnego kodu złośliwego oprogramowania, umożliwiający jego analizę wsteczną (reverse engineering).
- Otwarte środowisko programowania (API) umożliwiające integrację z najlepszymi systemami typu SIEM, takimi jak aplikacje Palo Alto Networks dla Splunk lub innymi rozwiązaniami bezpieczeństwa.

Taka analiza dostarcza wskaźników (IOC – Indication of Compromise), które można wykorzystać w każdym elemencie łańcucha ataku.

Utrzymanie prywatności plików
WildFire wykorzystuje publicznie dostępne rozwiązania chmurowe udostępniane przez Palo Alto Networks. Wszystkie podejrzane pliki są przesyłane poprzez bezpieczny kanał i firewalle do bazy WildFire, a połączenie z obu stron jest szyfrowane i podpisywane przez Palo Alto Networks. Wszystkie przesłane pliki są kasowane, a złośliwy kod jest ekstrachowany dla późniejszej analizy.

Wymagania systemowe WildFire:
- Do korzystania z systemu WildFire wymagany jest system PAN-OS™ 4.1+
- DF, Java, Office oraz mechanizm analizy APK wymaga systemu PAN-OS 6.0+
- analiza stron internetowych oraz mechanizmów korzystających z Adobe Flash wymaga systemu PAN-OS 6.1+

Informacje odnośnie licencji:
Podstawowe funkcjonalności oferowane przez system WildFire wymagają platformy działającej pod kontrolą systemu PAN-OS 4.1 lub nowszej.

- Analiza w systemach Windows XP i Windows 7
- Analiza plików wykonywalnych (EXE), bibliotek (DLL) oraz plików skompresowanych (ZIP) włącznie z materiałami przesyłanymi przez szyfrowany kanał (SSL)
- Automatyczne przesyłanie podejrzanych plików do systemu WildFire
- Automatyczne dostarczanie aktualizacji zabezpieczeń (wymagana licencja pozyskiwania zabezpieczeń) co 24 – 48 godzin.

Subskrypcja aktualizacji WildFire umożliwia ochronę niemal w czasie rzeczywistym, obejmując tym:

- Automatyczną aktualizację sygnatur wykrytego na całym świecie złośliwego oprogramowania w ciągu 15 minut.
- Rozszerzoną obsługę plików, obejmującą: pliki wykonywalne (pliki EXE, biblioteki DLL i inne), dokumenty pakietu Microsoft Office, pliki w formacie Portable Document Format (PDF), aplety Java (pliki JAR lub CLASS), pliki systemu Android (APK), aplety Adobe Flash (SWF oraz SWC), treść stron internetowych.
- Wsparcie dla urządzeń WF-500.
- Obsługę interfejsu programowania WildFire API pozwalającą na przesyłanie do 1000 próbek oraz 10000 raportów dziennie.

WF-500

WF-500 jest opcjonalnym urządzeniem pozwalającym użytkownikom WildFire na stworzenie prywatnej chmury bezpieczeństwa i ochrony danych. Urządzenie WF-500 zostało zaprojektowane w celu obsługi średnich lub dużych sieci, dając opcję obsługi dodatkowych urządzeń co pozwoli na sprawdzanie ruchu nawet w rozległych geograficznie sieciach.

SPECYFIKACJA WF-500

PROCESOR	PAMIĘĆ OPERACYJNA	DYSK SYSTEMOWY
Dwa 6-rdzeniowe procesory Intel z wbudowaną funkcją Hyper-Threading	128 GB pamięci operacyjnej	Dysk SSD o pojemności 20 GB

SPECYFIKACJA SPRZĘTU

WE/WY ORAZ PAMIĘĆ MASOWA	POJEMNOŚĆ	ZASILANIE
Ethernet: 4×10/100/1000 szeregowy port konsoli DB9 port USB do podłączenia do 2 TB pamięci masowej w postaci macierzy RAID	2 TB RAID1: do 4 certyfikowanych napędów o pojemności 1 TB	Dwa redundantne zasilacze o mocy 920 W w konfiguracji hot-swap
MAKSYMALNY POBÓR ENERGII	**MONTAŻ W SZAFIE RACK (WYMIARY)**	
510 Wat	2U, standardowa szafa rack 19" (3,5"H × 21"D × 17,5"W)	
MAX BTU/HR	**NAPIĘCIE WEJŚCIOWE (CZĘSTOTLIWOŚĆ WEJŚCIOWA)**	
1,740 BTU/hr	100 – 240 VAC (50 – 60 Hz)	
MAKSYMALNY POBÓR ENERGII	**BEZPIECZEŃSTWO**	
11 A @ 100 VAC	UL, CSA, CB	
EMI	**WYMAGANIA ŚRODOWISKOWE**	
FCC Class A, CE Class A, VCCI Class A	Temperatury pracy: od 32 do 95 °F, od 5 do 35 °C Temperatury przechowywania: od -4 do 95 °F, od -40 do 35 °C	

W celu zapoznania się z dodatkowymi informacjami odnośnie urządzenia WF-500 zapraszamy na stronę www.paloaltonetworks.com/products

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