TRAPS

Zaawansowana ochrona stacji roboczych

Palo Alto Networks® Traps™ to system zapewniający zaawansowaną ochronę stacji roboczych przed exploitami i nieznanymi atakami złośliwego kodu. Traps osiąga to poprzez wysoce skalowalnego, nieobciążającego zasoby agenta, korzystającego z innowacyjnego podejścia do obrony przeciw atakom, nie wymagającego wcześniejszej znajomości zagrożenia. Dzięki temu Traps udostępnia organizacjom potężne narzędzie chroniące stacje robocze przed niemal każdego rodzaju ukierunkowanym atakiem.

Zaawansowana ochrona stacji roboczych powinna umożliwiać:

- **Powstrzymywanie każdego rodzaju exploitów, włącznie z tymi wykorzystującymi podatności typu zero-day**
- **Powstrzymywanie wszelkiego rodzaju plików wykonywalnych ze szkodliwym kodem, bez wcześniejszej znajomości danego zagrożenia**
- **Zapewnianie szczegółowych informacji o powstrzymanych atakach**
- **Zapewnianie wysokiej skalowalności oraz minimalnego obciążenia dla systemu**
- **Zapewnianie bliskiej integracji z zabezpieczeniami sieciowymi oraz chmurowymi**

Pomimo szerokiej dostępności produktów zapewniających bezpieczeństwo, stacje robocze są nadal infekowane w zastraszającym tempie. Tradycyjne metody ochrony po prostu nie są w stanie nadążać za gwałtownie zmieniającym się krajobrazem zagrożeń (patrz: Rysunek 1). Zamiast sprawdzania i prób identyfikacji milionów pojedynczych ataków lub prób wykrywania złośliwych zachowań – co może okazać się niemożliwym – działanie Traps sprowadza się do bazowych technik, których każdy z atakujących musi użyć w celu przeprowadzenia skutecznego ataku. Dzięki takiemu podejściu Traps może udaremniać ataki zanim szkodliwy kod uzyska możliwość skutecznego wykonania się.

Różne rodzaje ataków, kompletna ochrona

Ataki przybierają różne formy i pojawiają się korzystając z różnych dróg, obejmujących zarażone strony www, pocztę elektroniczną lub zewnętrzne pamięci masowe. Większość dostępnych na rynku tradycyjnych rozwiązań zabezpieczających przed złośliwym oprogramowaniem chroni jedynie przed najmniej wyszukanymi jego odmianami. Niektóre z najbardziej wyrafinowanych i ukierunkowanych ataków przeprowadzane są z wykorzystaniem pozornie nieszkodliwych plików, które użytkownik otwiera korzystając z zatwierdzonych aplikacji. Przykładowo – złośliwy kod może zostać wbudowany w dokument programu Microsoft® Word® lub plik PDF – taka podatność nazywana jest exploitem. Traps chroni stacje robocze powstrzymując złośliwy

Rysunek 1: Błędy tradycyjnego podejścia do zagadnień bezpieczeństwa

kod przed wykonaniem i wykorzystaniem exploitów zarówno w postaci plików, jak i dostępnych poprzez sieć.

Najbardziej zaawansowane dzisiejsze zagrożenia wykorzystują błędy w oprogramowaniu, którego używamy na co dzień. Często pojawiają się w znanych typach plików (np. PDF, RTF, DOC, PPT, XLS) lub mogą brać na cel konkretne oprogramowanie wykorzystywane w różnych firmach.

Po uruchomieniu zarażonego pliku złośliwy kod wykorzystuje podatności w znanych aplikacjach użytych do otwarcia danego pliku, pozwalając jednocześnie na wykonanie własnego kodu i przejęcie pełnej kontroli nad zarażoną stacją roboczą.

Jak działa zapobieganie wykorzystaniu exploitów

Niezależnie od typu lub kompleksowości ataku, atakujący musi uruchomić sekwencję operacji pozwalającą na wykorzystanie luk w oprogramowaniu. Niektóre typy ataków wymagają więcej kroków, niektóre mniej; niemniej jednak we wszystkich przypadkach wymagane jest użycie przynajmniej dwóch lub trzech technik w celu skutecznego przejęcia kontroli nad atakowaną stacją. Traps wykorzystuje zestaw modułów profilaktycznych łagodzących lub powstrzymujących różne techniki dostępne dla atakujących. Dodatkowo atak wymaga użycia konkretnych technik umożliwiających skuteczne wykorzystanie exploita. Traps sprawia, że te techniki stają się całkowicie bezużyteczne, co oznacza, że aplikacja nie jest dalej podatna na złośliwy kod.

Traps wstrzykuje własny kod w każdy uruchamiany proces. Jeżeli proces próbuje użyć jednej z technik ataku, próba wykorzystania exploita nie powiedzie się ponieważ Traps uodpornił działające procesy. Traps natychmiastowo blokuje proces wykorzystujący techniki ataku oraz informuje zarówno użytkownika, jak i administratora o podjętych krokach i raportuje wszystkie działania do managera zabezpieczeń (patrz: Rysunek 2). Ze względu na łańcuchową naturę wykorzystywania exploitów, powstrzymanie działania jednego z ogniw pozwala na blokadę całego ataku.

Domyślnie polityki systemu Traps kontrolują ponad 100 procesów, a każdy z nich jest sprawdzany z użyciem odpowiednich modułów zapobiegania wykorzystaniu exploitów (Exploit Prevention Modules). W przeciwieństwie do innych rozwiązań, Traps nie jest ograniczony do ochrony wyłącznie wybranych procesów lub aplikacji.

Koncentrując się nie na samych technikach ataku Traps umożliwia powstrzymanie go bez wcześniejszej znajomości zagrożenia, niezależnie od znanych podatności, sygnatur zagrożeń lub aktualizacji oprogramowania. Należy podkreślić, że Traps nie dokonuje skanowania lub monitoringu uruchomionych procesów, wobec czego ochrona wykorzystuje bardzo małą ilość zasobów procesora lub pamięci operacyjnej.

Zapobieganie wykonywaniu złośliwego kodu

W celu zapobiegania wykonywaniu złośliwego kodu i zapewnienia pełni bezpieczeństwa, Traps wykorzystuje wielowarstwowe techniki skupiające się na trzech podstawowych zakresach wykorzystywanych przez złośliwe oprogramowanie. Kombinacja tych technik oferuje skuteczne metody zapobiegania zagrożeniom obejmujące takie techniki, jak:

1. **Restrykcje bazujące na politykach działania:** W organizacjach możliwa jest konfiguracja polityk zabezpieczeń opartych na specyficznych scenariuszach. Przykładowo, możliwe jest zablokowanie uruchamiania plików tymczasowych przez program Outlook lub zablokowanie uruchamiania określonych typów plików z dysków podpiętych do portów USB.

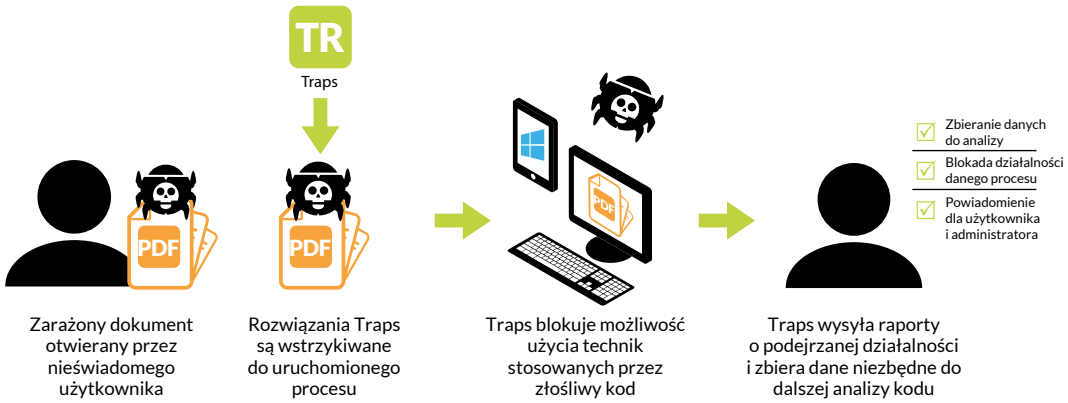
2. **Zaawansowana kontrola plików wykonywalnych:** Traps zapewnia również kontrolę procesów potomnych, sprawdza zawartość folderów, nieprzypisanych plików wykonywalnych, jak również zbiera dane umożliwiające precyzyjną kontrolę nad aplikacjami oraz zdefiniowanie, które aplikacje powinny mieć możliwość działania.

3. **Inspekcja oraz analiza mechanizmem WildFire™:** Mechanizm Traps przygotowuje kolejkę nieznanych plików wykonywalnych (.exe) do sprawdzenia i oceny zagrożenia przez narzędzie WildFire.

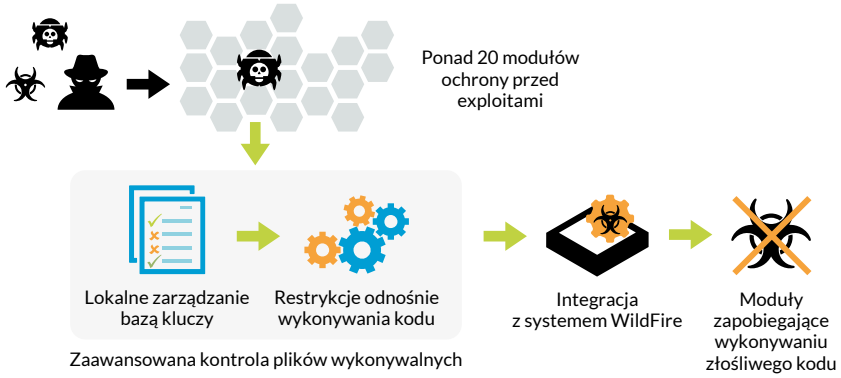
4. **Techniki ograniczania działalności złośliwego kodu:** Rozwiązania Traps implementują techniki blokowania wykonywania złośliwego kodu poprzez analizę danych wstrzykiwanych w uruchomione procesy.

Analiza śledcza

Ilość danych zebranych wskutek nieudanego ataku jest znacząco niższa niż ilość informacji, którą można zebrać po udanym naruszeniu polityk bezpieczeństwa. Mimo wszystko pozwala nadal na zebranie



Rysunek 2: Powstrzymywanie zagrożeń – od strony użytkownika



Rysunek 3: Poprawna metoda zapobiegania wykonywaniu złośliwego kodu

szerokiego zakresu informacji. Zebrane podczas próby ataku dane pozwalają na wdrożenie aktywnej ochrony dla dotychczas niechronionych stacji roboczych.

Dane o próbach ataków zbierane są przez oprogramowanie Traps. Agent oprogramowania Traps zbiera informacje o każdym uruchomionym procesie i przesyła owe informacje do managera zabezpieczeń (Endpoint Security Manager). Po powstrzymaniu ataku następuje zbieranie danych z danej stacji roboczej, włącznie z pełnym zgraniem stanu pamięci oraz informacji o działaniach, które próbował przeprowadzić złośliwy kod.

Traps udostępnia mechanizmy monitorowania aktywności według plików, folderów lub kluczy rejestru rozciągając proces przeszukiwania na wszystkie stacje robocze, co z kolei wspomaga analizę przeprowadzanych ataków.

Architektura wdrożeniowa Traps

Konsola managera zabezpieczeń stacji roboczej

Infrastruktura Traps obsługuje wiele różnych architektur, pozwalając na korzystanie z różnych, skalowalnych środowisk. Instalacja managera zabezpieczeń wiąże się z uruchomieniem bazy danych wykorzystującej rozwiązania Microsoft SQL Server® oraz konsoli administracyjnej korzystającej z serwera IIS. Obsługiwane są bazy danych Microsoft SQL 2008, 2012 i 2014 oraz możliwe jest wykorzystanie istniejącej bazy serwera SQL.

Konsola managera zabezpieczeń serwera

Serwery zabezpieczeń stacji roboczych działają w praktyce jako serwery proxy pomiędzy agentami Traps, a bazą danych serwera ESM (Endpoint Security Manager). Komunikacja pomiędzy agentami Traps i serwerami ESM odbywa się z wykorzystaniem protokołu HTTPS. Serwery ESM nie przechowują żadnych danych, dzięki czemu mogą być w razie potrzeby w prosty sposób dodawane lub usuwane z danego środowiska, celem zapewnienia odpowiedniego pokrycia geograficznego i wymaganej redundancji.

Agent Traps

Agent systemu Traps zawiera się w 9MB pakiecie MSI, który może być rozprowadzany wraz z innymi aktualizacjami. Dalsze aktualizacje oprogramowania agenta mogą być dostarczane poprzez konsolę zabezpieczeń stacji roboczej. Agent zabezpieczeń zużywa do 25 MB miejsca na dysku oraz do 40 MB pamięci operacyjnej. Obserwowane wykorzystanie czasu procesora mieści się w granicach 0,1%. Agent zabezpieczeń wykorzystuje różne metody uniemożliwiające jego wyłączenie przez użytkownika lub złośliwy kod.

Nieobciążająca zasobów struktura pozwala na skalowanie rozwiązań Traps tak, by możliwa była obsługa nawet dużych jednostek, obejmujących do 10 000 agentów zarządzanych z pojedynczej konsoli, wraz ze stałym utrzymywaniem scentralizowanej bazy danych polityk zabezpieczeń. Rozwiązania Traps mogą funkcjonować współbieżnie z innymi rozwiązaniami zabezpieczającymi, stale zapewniając bardzo niskie obciążenie procesora i urządzeń wejścia/wyjścia. Tak niskie obciążenie zasobów sprawia, że Traps jest idealnym rozwiązaniem dla krytycznych punktów infrastruktury, wysoko wyspecjalizowanych systemów lub środowisk wirtualnych.

Zewnętrzne systemy logowania

Konsola zarządzania, poza wewnętrznym sposobem zapisu danych, umożliwia logowanie do innych platform, takich jak SIEM lub obsługujących formaty CEF lub LEEF. W organizacjach wykorzystujących różne systemy konsol zarządzania, eksport zapisanych logów daje możliwość wykorzystania zewnętrznych narzędzi do agregacji i przeglądu zapisanych danych. Jako opcja dostępny jest mechanizm przesyłania informacji o krytycznych zdarzeniach z wykorzystaniem poczty elektronicznej.

Obsługiwane platformy systemowe

Traps pozwala na ochronę wielu systemów działających pod kontrolą systemu Microsoft Windows® – zarówno stacji roboczych, jak i serwerów, terminali, maszyn wirtualnych lub systemów korzystających z rozwiązań wbudowanych. Traps jest systemem w minimalnym stopniu obciążającym zasoby, co sprawia że jest idealnym rozwiązaniem dla wysoko wyspecjalizowanych systemów wykorzystywanych w takich zastosowaniach, jak: bankomaty, systemy POS, SCADA i wiele innych systemów przemysłowych, wymagających nieinwazyjnej ochrony uruchomionych procesów.

W CHWILI OBECNEJ TRAPS OBSŁUGUJE NASTĘPUJĄCE ROZWIĄZANIA:

SYSTEM OPERACYJNY
Windows XP (32-bit, Service Pack 3 lub nowszy)
Windows Vista (32-bit, 64-bit, z Service Pack 2)
Windows 7 (32-bit, 64-bit, RTM wraz z Service Pack 1; wszystkie edycje z wyjątkiem wersji Home)
Windows 8 (32-bit, 64-bit)
Windows 8,1 (32-bit, 64-bit)
Windows 10 (32-bit, 64-bit)
Windows Server 2003 (32-bit, Service Pack 2 lub nowszy)
Windows Server 2003 R2 (32-bit, Service Pack 2 lub nowszy)
Windows 2008 (32-bit, 64-bit)
Windows Server 2012 (wszystkie edycje)
Windows Server 2012 R2 (wszystkie edycje)

ŚRODOWISKA WIRTUALNE
Virtual Desktop Instance (VDI)
Maszyny wirtualne (VM)
Citrix, VMware, VirtualBox oraz Parallels
PLATFORMY SPRZĘTOWE
Komputery, serwery oraz tablety pracujące pod kontrolą systemu Windows
Systemy ICS oraz SCADA
Bankomaty (ATM) oraz systemy POS
OBSŁUGA PRZEGLĄDAREK
Internet Explorer 10 lub nowszy
Chrome 27 lub nowszy
Firefox 22 lub nowszy
Opera 12 lub nowsza

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

© 2015 Palo Alto Networks, Inc. Palo Alto Networks są znakiem towarowym zastrzeżonym przez Palo Alto Networks. Listę zastrzeżonych przez nas znaków towarowych można znaleźć na stronie internetowej http://www.paloaltonetworks.com/company/trademarks.html. Wszystkie inne znaki towarowe wymienione w niniejszym dokumencie są znakami towarowymi zastrzeżonymi przez odpowiednie firmy.