Palo Alto TRAPS 4.0
Co nowego?

Opracowanie własne (listopad 2017)

1. Ochrona przed plikami Microsoft Office

System Traps w wersji 4.0 został wzbogacony o funkcjonalność ochrony przed szkodliwymi makrami zawartymi w plikach Microsoft Office. Zawiera on moduły ochrony w plikach:

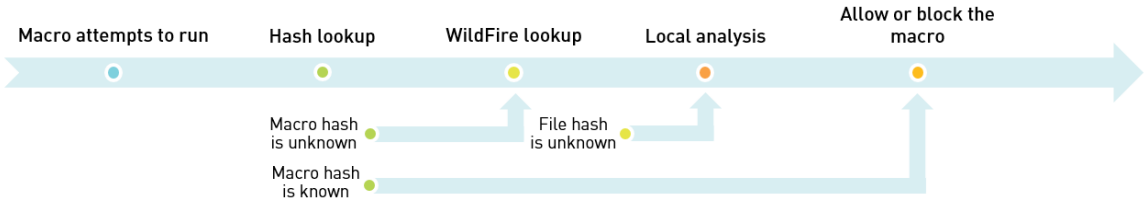
- Microsoft Office 2003 – 2007 – doc, xls
- Microsoft Office 2010 i nowsze – docm, docx, xlsm, xlsx

Na samym początku weryfikowany jest skrót SHA256 makra względem lokalnego cache. W przypadku gdy mamy już werdykt (niezależnie od tego czy pochodzi on z WildFire czy ręcznie wprowadzonego przez administratora wpisu) Traps zachowuje się zgodnie z jego wartością – blokuje lub zezwala na wykonanie kodu w makrze.

Jeżeli werdykt nie jest znany, równolegle odbywają się dwie czynności:

- **Kod makra** jest poddawany mechanizmowi lokalnej analizy, która wykonuje analizę z wykorzystaniem zarówno mechanizmów Machine Learning jak i statycznej analizy kodu.
- Równolegle **makro** jest wysyłane do chmury WildFire celem analizy.

Co najważniejsze, wysyłane jest jedynie makro – treść dokumentu nie opuszcza stacji roboczej i nie jest wysyłana nigdzie na zewnątrz. W przypadku gdyby lokalna analiza nie wykryła nic podejrzanego, zawsze działają pozostałe moduły Exploit Protection Module które mają za zadanie chronić proces programu przed podejrzanymi czynnościami lub metodami które wykorzystywane są podczas przeprowadzania ataków.



Przebieg procesu weryfikacji makra w plikach Microsoft Office

2. Uproszczony mechanizm licencjonowania

W odpowiedzi na sugestie i prośby użytkowników oraz partnerów, nastąpiła zmiana mechanizmu licencjonowania systemu Traps. Od teraz, wszystkie typy licencji agenta (Workstation/Server/VDI) zostały zintegrowane w jedną pulę, dzięki czemu nie musimy się

martwić o liczbę chronionych stacji roboczych lub serwerów posiadając wolne licencje na system niewłaściwego typu.

3. Agent Traps dla systemu Mac OS

Od wersji 4.0 dostępny jest agent Traps na platformę macOS, rozszerzając ochronę na stacje robocze z tym systemem operacyjnym. Wspierane systemy to OS X 10.10 (Yosemite) i nowsze.

Unikalną funkcjonalnością dedykowaną dla platformy macOS jest **Gatekeeper Enhancement MPM** oraz **DyLib-Hijacking Protection**. Pierwsza z nich pozwala na rozszerzenie funkcjonalności Gatekeeper o ochronę przed uruchomieniem niepodpisanych procesów potomnych poprzez zaufaną aplikację. Od teraz, możemy decydować również o poziomie podpisu procesów potomnych (np. zezwalamy na procesy podpisane przez Apple System, Mac App Store, blokujemy Developers).

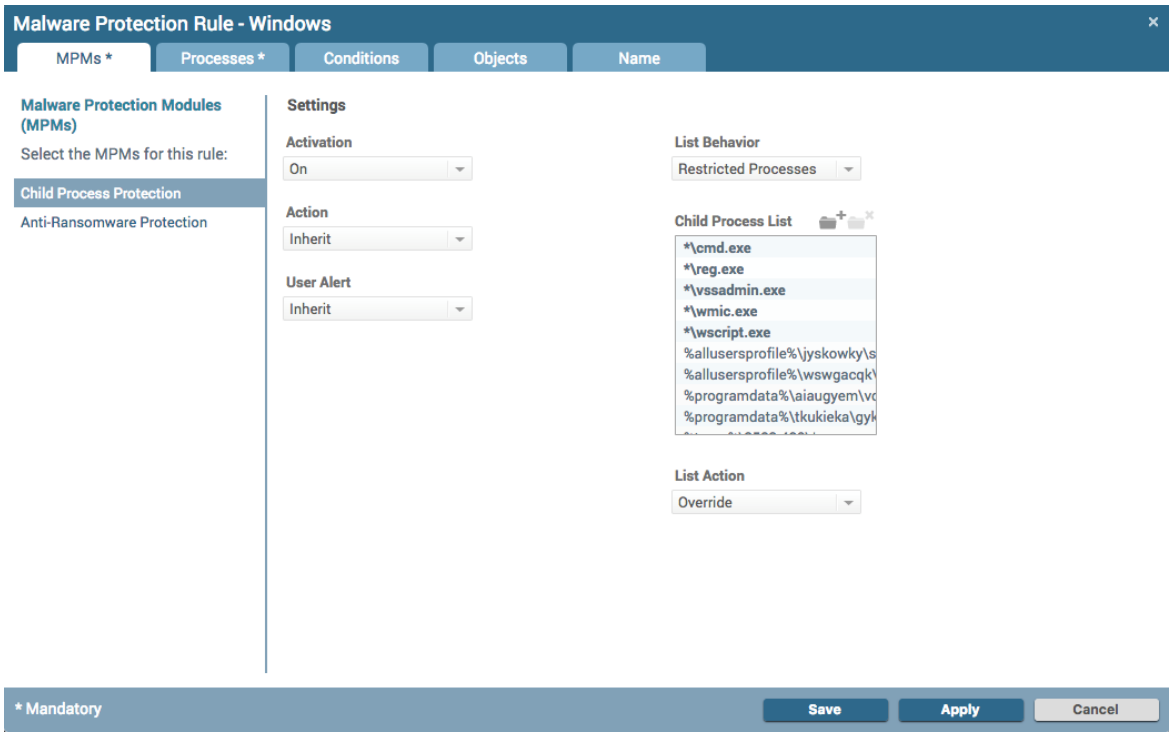
Moduł DyLib-Hijacking Protection wprowadza ochronę przed załadowaniem nieautoryzowanych bibliotek dynamicznych (dylib) wykorzystujących atak na technikę ich wyszukiwania – poprzez używanie wieloznacznych ścieżek w mechanizmie wyszukiwania bibliotek oraz uprawnienia zapisu plików do katalogu aplikacji i standardowych katalogów z bibliotekami. Moduł ten jest domyślnie uruchomiony i zabezpiecza nas przed tego typu atakami nawet jeżeli proces lub użytkownik ma pełne uprawnienia do tych katalogów.

Wersja 4.1 udostępnia również mechanizm lokalnej analizy dla systemu macOS, który jest uzupełnieniem mechanizmu dynamicznej analizy plików oferowanej przez platformę WildFire.

4. Zaawansowana kontrola nad procesami potomnymi

Wersja 4.0 wprowadza usprawnienia do ochrony przed procesami potomnymi. Mamy do dyspozycji nowy moduł **Malware Protection Module (MPM)**, za pomocą którego administrator może zdefiniować listę procesów potomnych jako tzw. whitelistę (czyli zezwalamy jedynie na wykonywanie procesów znajdujących się na liście) lub tzw. Blacklistę (czyli zezwalamy na uruchamianie wszystkich procesów za wyjątkiem tych znajdujących się na liście).

Wersja 4.1 wprowadza kolejne ulepszenia do modułu. Mamy teraz pełną kontrolę nad procesami uruchamianymi z linii komend (np. za pomocą cmd.exe, powershell.exe a także hosta skryptów Windows Scripting Host i hosta usług Windows – svchost.exe). Możemy definiować polityki np. zawsze blokujące uruchomienie procesu powershell.exe poprzez Microsoft Word, zezwalając na uruchamianie innych (np. cmd.exe). Dodatkowo, możemy zezwolić lub zabronić uruchomienia procesu na podstawie jego lokalizacji – czyli proces powershell.exe uruchomi się jedynie jeśli znajduje się w domyślnej lokalizacji systemowej i jest zweryfikowany cyfrowo, zaś inny proces powershell.exe znajdujący się np. w C:\Downloads nie zostanie uruchomiony (nawet pomimo prawidłowego podpisu cyfrowego).



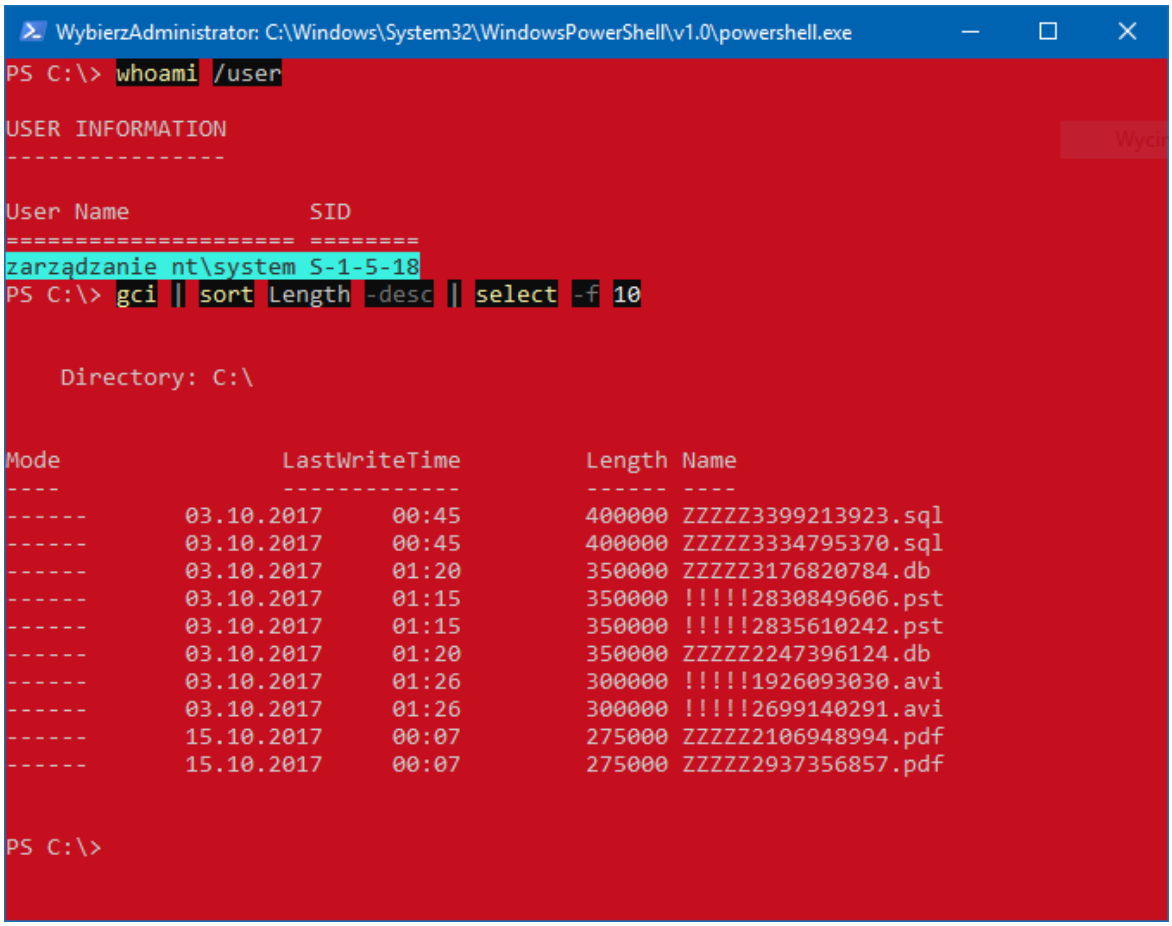
Konfiguracja ochrony procesów potomnych

5. Moduł AntiRansomware Protection

Od wersji 4.1 wprowadzony został dedykowany, zaawansowany moduł przeciwko oprogramowaniu typu ransomware, które szyfrują pliki na dysku oraz żądają okupu za ich odzyskanie.

Przeprowadzając atak typu Ransomware, atakujący najczęściej korzysta z dedykowanego pliku binarnego, wykorzystuje biblioteki DLL, makra lub skrypty powłoki systemowej. Ochrona przed tego typu atakami była zapewniona już wcześniej, dzięki modułom Exploit Protection Modules, Malware Protection Modules, restrykcjom, ochronie procesów potomnych oraz integracją z WildFire.

Jako dodatkową warstwę ochrony, agent Traps tworzy w kilkunastu folderach (m. in katalogu głównym, na pulpicie, w dokumentach etc.) **niewidoczne** dla użytkownika pliki o najpopularniejszych rozszerzeniach (obrazy, dokumenty, ale także np. klucze prywatne, certyfikaty cyfrowe i bazy danych), których istnienia nie jest on nawet świadomy. Pliki te działają jak mechanizm honeypot – wszelkie manipulacje tymi plikami i operacje na nich są ściśle monitorowane. W przypadku wykrycia niepożądanych akcji, agent Traps natychmiast blokuje proces który dokonał zmian, co efektywnie zabezpiecza nas przed atakami typu Ransomware.



Pliki typu honeypot widoczne w katalogu C:\ jako użytkownik NT AUTHORITY\SYSTEM

6. Ochrona przed fingerprintingiem z wykorzystaniem Exploit Kitów

Nowy moduł Exploit Protection Module (EPM) o nazwie **Exploit Kit Fingerprinting Protection** zapewnia nam ochronę przed procesem fingerprintingu, czyli pozyskiwania informacji o środowisku, która ma za zadanie usprawnić proces ataku poprzez identyfikację podatności, wgląd w zainstalowane oprogramowanie lub aktualnie zalogowanego użytkownika.

Moduł ten działa na zasadzie wykrywania zachowań które są charakterystyczne dla oprogramowania generowanego przez popularne Exploit Kity, np. Metasploit Framework. Exploit Kity także mogą być uruchamiane jako witryna sieci WWW, dlatego domyślna polityka zakłada automatyczną ochronę dla popularnych przeglądarek Internetowych.

7. Ochrona przed eskalacją uprawnień na poziomie jądra systemu operacyjnego

Moduł ten zabezpiecza przed atakami mającymi na celu eksploitację jadra systemu operacyjnego poprzez ochronę przez załadowaniem złośliwego kodu (shellcode) i jego wykonania. System Traps monitoruje wszelki dostęp do pamięci która nie jest zamapowana, co pozwala na zablokowanie zagrożenia bez szkody dla procesu który został wykorzystany w celu wykorzy

Dodatkowo, poprzez integrację z wyżej opisanym mechanizmem, moduł ten potrafi rozpoznać ataki wykonywane przez Exploit Kity i narzędzia np. DoublePulsar czy EternalBlue – które to w głównej mierze odpowiadały za lawinę ataków typu WannaCry, wykorzystujących szereg podatności w protokole SMBv1.

W wersji 4.1 moduł ten został udoskonalony o ochronę APC (Asynchronous Procedure Call), eliminując ryzyko uzyskania dostępu do shellcode'u ze specyficznego adresu pamięci poprzez przekazanie wywołania APC z właściwej procedury.

8. Rejestracja w Microsoft Security Center

Od wersji 4.0, produkt Traps spełnił oficjalne warunki definicji oprogramowania antywirusowego założone przez Microsoft, przez co program Microsoft Security Center raportuje instalację agenta jako pełnoprawne rozwiązanie antywirusowe. Pozwala to na monitoring zabezpieczeń stacji roboczej za pomocą domyślnego narzędzia wbudowanego w systemy Microsoft Windows od 7 w górę.

Microsoft Security Center na bieżąco weryfikuje stan działania agenta Traps i status ochrony, co pozwala na podniesienie alarmu np. w przypadku wyłączenia integracji z platformą WildFire, program Microsoft Security Center ostrzeże nas że nie działa ochrona przed wirusami.

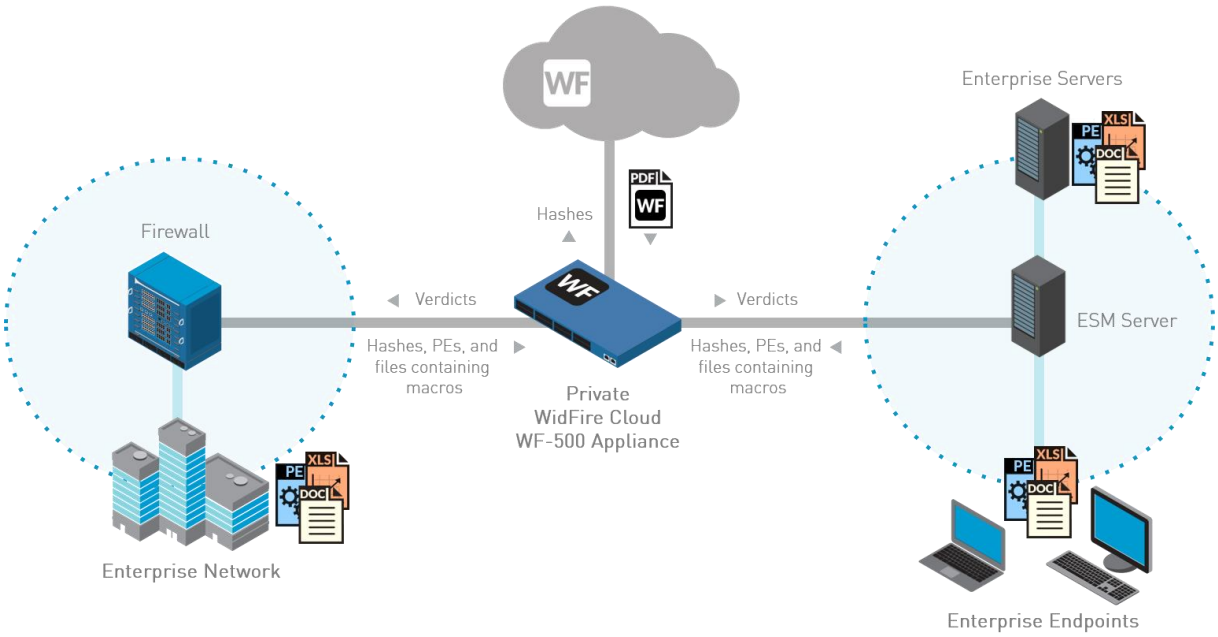
Agent Traps nie zostaje zarejestrowany w Microsoft Security Center dopóki nie otrzyma polityki z serwera zarządzania.

9. Wsparcie dla urządzenia WF-500

Platforma Traps 4.0 dodaje wsparcie dla dedykowanego urządzenia typu WildFire Private Cloud - Palo Alto Networks WF-500. Dzięki temu, posiadając takie urządzenie, możemy przeprowadzać analizę plików za jego pomocą, nie będąc zależnym od połączenia internetowego.

Urządzenie WF-500 obsługuje do 40,000 agentów Traps i jest idealnym rozwiązaniem w organizacjach, które są obostrzone regulacjami które efektywnie uniemożliwiają transfer plików poza granicę organizacji.

W domyślnej konfiguracji urządzenie WF-500 nie wysyła plików do chmury WildFire, jednak informacje o werdykcie są upubliczniane – dzięki czemu wszyscy klienci, którzy posiadają aktywną subskrypcję WildFire na firewallu Palo Alto Networks lub posiadają instalację Traps będą informowani o werdykcie dla danego pliku.



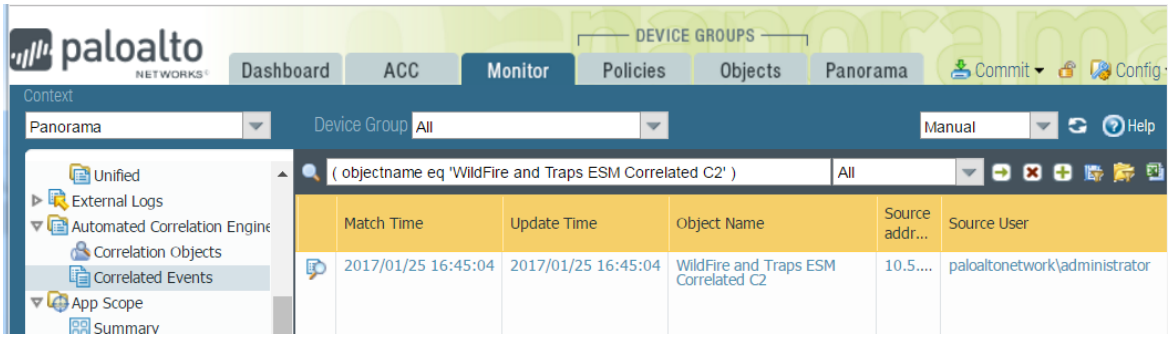
Przykładowy model wdrożenia z wykorzystaniem urządzenia WF-500

10. Integracja z systemem Panorama

Wersja Traps 4.0 wprowadza także możliwość przekazywania logów do systemu Panorama, który odpowiada za zarządzanie infrastrukturą systemów Palo Alto Networks, agregacją logów oraz korelacją zdarzeń.

System Panorama zapewnia nam analizę logów aktywności z całej infrastruktury sieciowej za pomocą pojedynczego panelu zarządzania. Pozwala nam to na łatwe monitorowanie stanu sieci i stacji roboczych oraz wprowadzi szerszy kontekst oraz widoczność w przypadku wykrycia zagrożenia. Widzimy punkt wejścia, wszelkie czynności, jak również komunikację sieciową – z szczególnym wskazaniem wszelakich adresów, portów i aplikacji, a także zrzutem pakietów komunikacji sieciowej.

Dzięki temu że Panorama posiada system automatycznej korelacji zdarzeń oraz posiada wsparcie dla pluginów do systemów zarządzania infrastrukturą (np. VMware NSX), możliwe jest także zautomatyzowane podjęcie czynności naprawczych, np. zablokowanie ruchu poprzez automatyczną modyfikację polityki bezpieczeństwa urządzeń firewall, przełączenie zainfekowanej stacji roboczej do innego segmentu sieci (np. inny VLAN) lub wręcz komunikację z warstwą orkiestracji infrastruktury i automatyczne przywrócenie serwera z migawki/kopii zapasowej lub wykreowanie nowej maszyny wirtualnej w miejsce zainfekowanej.



Automatyczna korelacja zdarzeń w systemie Panorama