

JAK NETASQ MINIMALIZUJE LICZBĘ FALSE POSITIVE

Silnik IPS firmy NETASQ łączy kilka zaawansowanych technologii, dzięki czemu jego współczynnik błędnej klasyfikacji wynosi mniej niż 1/100 000 (0,001 %).

Technika, dla której współczynnik błędnej klasyfikacji jest najwyższy, to skanowanie na podstawie sygnatur stosowane w tradycyjnych systemach IPS. Łącząc kilka rodzajów skanowania, technologia ASQ skutecznie walczy z błędną klasyfikacją:

Automatyczne wykrywanie protokołu zapewnia prawidłowe skanowanie na poziomie warstwy 7. Tradycyjne skanowanie oparte na sygnaturach może prowadzić do błędnego wskazania ataku sieciowego w tekście przesyłanym przez sieć lub pocztę e-mail, co jest spowodowane brakiem kontekstu przy ocenie sygnatury (patrz poniżej).

Ochrona oparta na protokole: Nieprawidłowe zastosowanie sygnatur, kiedy wymagana jest znajomość protokołu, zwiększa ryzyko błędnej klasyfikacji. Na przykład skanowanie oparte na sygnaturach daje wysokie ryzyko błędnej klasyfikacji w przypadku ataku polegającym na przepełnienia bufora (Buffer overflow). Poniżej znajduje się przykład sygnatury systemu open-source do zapobiegania włamaniom o nazwie Snort do wykrywania przepełnienia bufora FTP:

GEN:SID	1:341
Message	FTP EXPLOIT overflow
Rule	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 21 (msg:"FTP EXPLOIT overflow"; flow:to_server,established; content:"XXXXXX"; classtype:attempted-admin; sid:341; rev:6)

Niektóre sygnatury można bardzo łatwo błędnie sklasyfikować jeśli ich analiza opiera się tylko o sprawdzenie czy dana sygnatura występuje w analizowanym pakiecie. Dlatego też kiedy jest to bardziej wskazane, silnik IPS firmy NETASQ korzysta z tysięcy analiz protokołu, co gwarantuje bardzo niski współczynnik błędnej klasyfikacji.

Kilka typów analizy behawioralnej zastępuje mniej skuteczną analizę opartą na sygnaturach. Dla przykładu, wykrycie ukrytego kanału ping ICMP wymaga tylu sygnatur, ile jest programów ukrytych kanałów. Silnik IPS firmy NETASQ wykrywa i skutecznie blokuje te kanały dzięki analizie behawioralnej (proszę zwrócić uwagę, że ICMP ECHO payload = ICMP REPLY payload).

Sygnatury firmy NETASQ opierają się na normalizacji protokołu. Umożliwia to skuteczną walkę z włamaniami oraz różnymi niepożądanymi zdarzeniami na poziomie aplikacji. Na przykład: ruch http jest dekodowany (utf8, % kodowanie...) i normalizowany przed skanowaniem pod kątem ataków.

Ponad 30 kontekstów protokołu pozwala skupić się przy wykrywaniu zagrożeń na części skanowanego ruchu (żądanie lub odpowiedź SIP, parametr URL, konkretny nagłówek URL itp.). Daje to wielkie korzyści w porównaniu ze standardową analizą opartą na sygnaturach.

W przeciwieństwie do większości znanych sygnatur, które koncentrują się na wykrywaniu znanych ataków (nadużyć), **sygnatury kontekstowe skupiają się na lukach** i wykrywają nietypowe zachowanie. Przy braku jakiegokolwiek kontekstu może to prowadzić do zwiększenia ryzyka błędnej klasyfikacji: zachowanie nietypowe dla jednego protokołu lub konkretnej jego części może być całkowicie typowe dla innego protokołu.

Tradycyjna analiza oparta na sygnaturach skupia się na wykrywaniu ataku. Technologia NETASQ, wykorzystująca sygnatury kontekstowe, pozwala na skuteczniejsze wykrywanie luk i likwiduje konieczność tworzenia tysięcy sygnatur ataków: jako że każdej sygnaturze towarzyszy ryzyko błędnej klasyfikacji, wyeliminowanie tych zbędnych sygnatur znacząco zmniejsza liczbę fałszywych wskazań. Jednocześnie należy wskazać niski wpływ na wydajność pracy tego rozwiązania.

Automatyczne profile konfiguracyjne przeznaczone do konkretnych celów umożliwiają precyzyjną konfigurację. Pozwala na ustawienie przez administratora odpowiedniego poziomu bezpieczeństwa w zależności od kierunku ruchu.