

WHITE PAPER

JAK POZBYĆ SIĘ SPAMU Z MFILTRO

„NETASQ MFILTRO ma jeden z najwyższych wskaźników wykrywalności spamu na rynku, a w naszych testach nie miał ani jednego przypadku błędnej klasyfikacji.”

(DataNews 7 września 2007 r.)

CEL NINIEJSZEGO DOKUMENTU

W przypadku rozwiązań antyspamowych ich dostawcy kładą największy nacisk na skuteczność i łatwość obsługi. Niniejszy dokument przedstawia szczegóły zastosowania różnych technologii w NETASQ MFILTRO.

TECHNIKI ANTYSZPAMOWE

Polityka antyspamowa zastosowana w MFILTRO składa się z dwóch części:

- kontekstu wiadomości e-mail - poziom protokołu,
- treści wiadomości e-mail - poziom danych.

W skład **pierwszej części** wchodzi wszystkie reguły funkcjonujące w czasie połączenia SMTP na poziomie protokołu. Spośród tych technologii NETASQ MFILTRO stosuje Reputację IP – dynamiczne listy RBL, dynamiczne listy URLBL, lokalne białe i czarne listy IP. Do blokowania skryptów spamu służy wczesne wykrywanie talkerów.

Do innych stosowanych technik zaliczyć można weryfikację aktualnej domeny opartą na zapisach MX i/lub A, białe i czarne listy domeny nadawcy i jego adresu e-mail, przetrzymywanie dynamicznych adresów IP itp.

Adresy e-mail odbiorców można sprawdzić za pomocą list lokalnych, weryfikacji SMTP RCPT bądź zapytań LDAP/Active Directory.

Wszystkie wymienione wyżej techniki funkcjonują na poziomie połączenia, co oznacza, że potencjalny spam nigdy nie przechodzi przez połączenie internetowe klienta. Przeciętnie **80% spamu jest zatrzymywane już na poziomie protokołu**. NETASQ MFILTRO nie tylko zwalnia zasoby na wewnętrznych serwerach pocztowych klienta, lecz również uwalnia pasmo, blokując 80% spamu nim dotrze on do połączenia internetowego.

Druga część polityki NETASQ MFILTRO dotyczy treści wiadomości e-mail. Silnik antyspamowy NETASQ MFILTRO bierze pod uwagę całą wiadomość e-mail, zarówno nagłówki jak i jej treść. Istnieje możliwość usunięcia załączników a także konfiguracji analizy treści wiadomości opartej na słowach lub zdaniach.

Ta metoda filtrowania heurystycznego opiera się na kilku tysiącach reguł różnego typu, z których wszystkie stosowane są dla wiadomości w celu osiągnięcia podstawowego rezultatu.

Reguły heurystyczne mają charakter doświadczalny i nie można ich przewidzieć. Powstają na podstawie zaawansowanej analizy wszystkich części wiadomości:

1. nagłówków, ze szczególnym uwzględnieniem tematu,
2. zwykłego tekstu,
3. części HTML,
4. nazw załączników i ich treści.

Reguły heurystyczne tworzą eksperci, wynajdujący powtarzające się elementy różnych

wiadomości (zwłaszcza częściowo lub w całości generowanych przez roboty). Później wiadomości mające takie elementy są automatycznie uznawane za spam, niezależnie od ich tematu.

Tworzenie reguł heurystycznych wymaga perfekcyjnej znajomości wszystkich protokołów związanych z wiadomościami e-mail jak również szerokiej wiedzy praktycznej z zakresu działania spamu. W tym procesie ludziom pomagają komputery z dedykowanymi narzędziami, które rozwijały się wraz z samym filtrem. Nowe hipotezy są szybko sprawdzane na nowym spamie oraz istniejącym już korpusie. Reguły wyników negatywnych, choć rzadziej spotykane, mają nadrzędne znaczenie dla ograniczania ryzyka błędnej klasyfikacji wiadomości.

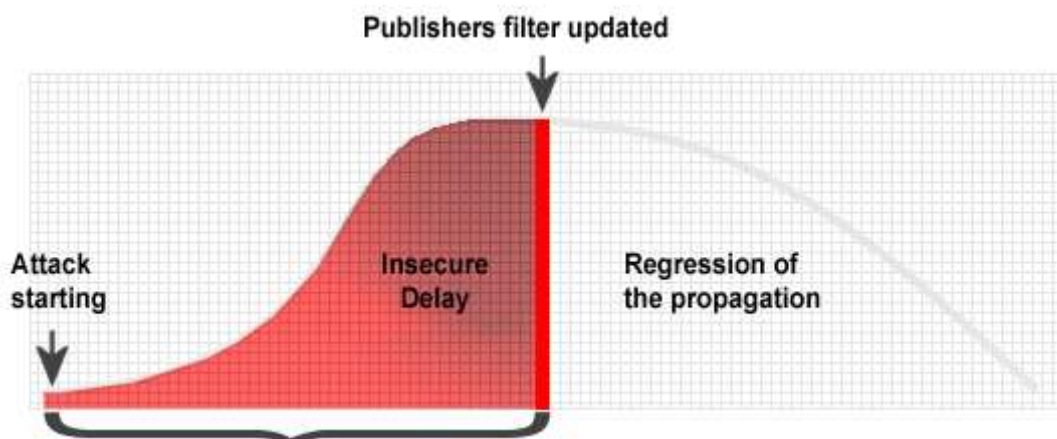
Dzięki zaawansowanemu filtrowi heurystycznemu technologia NETASQ MFILTRO może przewidywać niektóre niechciane wiadomości e-mail oraz wirusy zanim zdążą się one rozprzestrzenić. Ta innowacyjna funkcja zapewnia ochronę przed zupełnie nowym atakiem, podczas gdy inni producenci oprogramowania potrzebują czasu na zaktualizowanie swoich silników antyspamowych i antywirusowych.

ZAAWANSOWANY FILTR HEURTYSTYCZNY

Analiza heurystyczna to innowacyjny sposób skanowania wiadomości stworzony przez inżynierów NETASQ MFILTRO i jeden z głównych elementów silnika antyspamowego firmy NETASQ. Jest to odpowiedź na problemy producentów oprogramowania, którzy w chwili pojawienia się zagrożenia potrzebują pewnego czasu na interwencję.

Ataki wirusów są coraz częstsze i miewają coraz poważniejsze skutki. Kilka lat temu wirusy potrzebowały kilku dni lub tygodni by okrażyć świat. Obecnie wystarczy kilka godzin by zainfekować miliony stacji roboczych. Konie trojańskie i robaki stworzyły sieci (tzw. botnety), które umożliwiają spamowi i wirusom bardzo szybkie rozprzestrzenianie się po całym świecie.

Ataki są coraz bardziej niszczycielskie, więc producenci oprogramowania antywirusowego muszą reagować szybciej. Niemniej zawsze istnieje krytyczny okres braku ochrony. W tym czasie wirusy i niechciane wiadomości e-mail mogą być rozsyłane na tysiące komputerów.



Powyższy schemat prezentuje okres braku ochrony w trakcie ataku wirusów.

Dzięki Zaawansowanemu filtrowi heurystycznemu z funkcją przewidywania wyniku NETASQ MFILTRO chroni użytkowników od początku ataku.

Analiza heurystyczna umożliwia wykrywanie spamu oraz wirusów bez konieczności interwencji czy aktualizacji. Dzięki temu użytkownicy są chronieni nawet podczas tzw. okresu braku ochrony.

Niebezpieczne systemy, które do masowego rozprzestrzeniania się wykorzystują ukryte wejścia, mają jednak słaby punkt, ponieważ skupiają się na nowych wirusach lub na widocznej treści wiadomości. Stworzenie zainfekowanej wiadomości e-mail wymaga stosowania technik, które rozwijają się wolniej. Do zablokowania wiadomości z wirusem wystarcza inteligentna analiza jej struktury. Nie ma potrzeby analizy samego zainfekowanego pliku.

Praca nad systemem analizy heurystycznej polega na zachowaniu jedynie tych reguł, które oparte są na sekwencjach niepożądanych wiadomości e-mail o dużym prawdopodobieństwie ponownego pojawienia się. Za regułę heurystyczną uznaje się taką, która powstała w odpowiedzi na konkretny atak, ale reaguje także na nowe ataki.

INNE CECHY SILNIKA ANTYSZPAMOWEGO

Filtrowanie reaktywne

Filtrowanie reaktywne jest jedną z najbardziej zaawansowanych i skutecznych części silnika NETASQ MFILTRO. Ogólnie rzecz biorąc zakłada ono wykrywanie technik stosowanych przez spamerów by przechytrzyć filtry antyspamowe pierwszej generacji. Poniżej znajduje się lista technik antyspamowych pierwszej generacji, kontrtechnik stosowanych przez spamerów oraz technik MFILTRO, które mają z nimi walczyć:

Podstawowa technika antyspamowa: czarne listy witryn wskazywanych w linkach w wiadomościach

Odpowiedź spamerów: redundantne kodowanie łącz URL

Skuteczna ochrona MFILTRO: wykrywanie redundantnego kodowania łącz URL

Podstawowa technika antyspamowa: filtrowanie według sumy kontrolnej wiadomości

Odpowiedź spamerów: wstawienie losowego ciągu znaków w taki sposób, aby nie było dwóch identycznych wiadomości

Skuteczna ochrona MFILTRO: wykrywanie losowych ciągów znaków w wiadomościach

Podstawowa technika antyspamowa: analiza statystyczna (metodą Bayesiańską) połączeń wyrazowych

Odpowiedź spamerów: dodanie neutralnych słów, czytelnych lub o małym kontraście / zapisanych małą czcionką

Skuteczna ochrona MFILTRO: wykrywanie niepowiązanych sekwencji słów, nieczytelnego lub mało czytelnego tekstu, nadużywania małej czcionki

Podstawowa technika antyspamowa: filtrowanie według słów kluczowych

Odpowiedź spamerów: zmiany w pisowni, umożliwiające jednak odczytanie słowa zgodnie z fonetyką danego języka

Skuteczna ochrona MFILTRO: wykrywanie typowych zmian we wrażliwych słowach i tagach HTML

Silnik NETASQ MFILTRO może wykryć setki wariacji słów „viagra”, od V1AGR4 do VVIAAGGRRRIA czy VIGRA, z których żadne nie są jako takie przechowywane w pamięci.

Wzorce HTML

Za każdym razem, gdy przesyłana wiadomość RFC-822 ma część HTML (a obecnie zazwyczaj tak właśnie jest), MFILTRO oblicza niepowtarzalną sumę kontrolną kodu HTML (wzorzec HTML). Następnie porównuje go z listą znanych wzorców typowych dla generowanego spamu. Ta technika, połączona ze statystyką rozmiarów obrazów zawartych w wiadomości, zapewnia **szczególnie wysoką skuteczność filtrowania spamu składającego się w głównej mierze lub wyłącznie z obrazów online.**

Wykrywanie fałszywych znaczników czasu SMTP i innych części nagłówek

Wykrywanie fałszywego nagłówka „Otrzymano:” i innych wpisów w nagłówkach wiadomości z czasem okazało się główną metodą wykrywania spamu.

Antyscam

Scam przybiera różne formy, najczęściej są to ostrożnie sformułowane propozycje finansowe, mające na celu zwabienie adresata wiadomości do wzięcia udziału w rzekomym lukratywnym przedsięwzięciu inwestycyjnym. NETASQ MFILTRO posiada moduł poświęcony wyłącznie wykrywaniu scamu, jako że scam mailowy w niewielkim stopniu przypomina codzienny spam reklamowy.

TECHNIKI ANTYWIRUSOWE

NETASQ MFILTRO może stosować rozwiązania antywirusowe innych producentów. Stosowane są zarówno skaner Clam AV jak i skaner firmy Kaspersky. By maksymalnie zwiększyć skuteczność opisanych powyżej technik analizy heurystycznej, skaner Clam AV ściśle połączono z zaawansowanym silnikiem heurystycznym wykorzystywanym podczas analizy antyspamowej. Dzięki temu potrzebna jest tylko jedna aktualizacja sygnatur heurystycznych dla Clam AV i MFILTRO.

Oprócz silnika NETASQ MFILTRO w trakcie analizy wiadomości e-mail użyć można aplikacji antywirusowej firmy Kaspersky. Pozostawia to dużą swobodę w kwestii polityki: dla jednych domen zastosować można sam skaner Clam AV, dla innych tylko skaner firmy Kaspersky, a w przypadku jeszcze innych możliwe jest **zastosowanie obu dla podwójnej ochrony**.

Jako że NETASQ MFILTRO może wywoływać te aplikacje w ramach polityki, można tę opcję skonfigurować nie tylko na poziomie domeny, ale również na poziomie adresów e-mail, użytkowników czy grup protokołu LDAP, list lokalnych itp.

Ta elastyczność jest szczególnie przydatna w środowiskach typu Managed Services lub złożonych sieciach WAN.

NETASQ MFILTRO MTA

Serwer Poczty czy Mail Transfer Agent (MTA, Agent Przesyłania Poczty) jest unikatowym rozwiązaniem w NETASQ MFILTRO.

Standardowo wszystkie wiadomości przychodzące do MTA są przetwarzane zgodnie z konkretną polityką stosowaną dla grupy wiadomości, do której one należą (zwykle, lecz nie zawsze, opartej na domenie odbiorcy), a następnie są usuwane, poddawane kwarantannie, przechowywane lub kierowane do serwera pocztowego zgodnie z wynikiem

przetwarzania. Oznacza to dużą elastyczność. Dla przykładu przekierowanie wiadomości do innego adresata może być oparte na zapytaniu LDAP.

MTA to struktura zarządzająca regułami, stosowanymi do każdej grupy wiadomości. Konfiguracja przez konsolę graficzną dostępną z poziomu przeglądarki internetowej pozwala administratorowi systemu na łatwe zdefiniowanie i zastosowanie procesów przeprowadzanych dla każdej grupy wiadomości.

MTA może przechowywać kilka polityk dla ruchu pocztowego, podczas gdy tylko jedna jest aktywna w danym momencie. Sprawia to, że przełączenie się z jednej polityki na inną zajmuje zaledwie kilka minut, bez konieczności zatrzymywania MTA czy utraty wiadomości. Każda polityka ruchu pocztowego składa się z reguł, które są przetwarzane w określonej kolejności. MTA jest zazwyczaj konfigurowany przez graficzną konsolę, ale istnieje również możliwość ładowania i edytowania plików konfiguracyjnych w formacie XML. Zbiór włączonych reguł jest kompilowany w celu przyspieszenia działania całego systemu.

Poza aplikacjami Mail Firewall, wyjątkowość MTA polega na niesamowitej łatwości integracji NETASQ MFILTRO z istniejącą infrastrukturą wiadomości. Wiele funkcji, takich jak podszywanie się pod domeny, przekazywanie wiadomości do kilku serwerów pocztowych czy sprawdzanie konkretnych usług subskrybowanych przez odbiorcę, które zwykle wymagają kodowania lub oskryptowania, jest tylko kwestią wskazania i kliknięcia w konsoli graficznej. Co więcej, bogate możliwości MTA pozwalają NETASQ MFILTRO replikować dowolną starszą, złożoną usługę pocztową, włączając warunkową transkrypcję adresu odbiorcy. Liczne funkcje kontrolujące ruch wychodzący od MTA do serwerów pocztowych zapewniają, że serwery nigdy nie będą przeciążone, ponieważ MTA może działać jako miejsce tymczasowego przechowywania wiadomości pocztowych, w czasie gdy klient konserwuje swoje serwery.

Zaawansowane reguły polityki mogą obejmować modyfikacje adresatów lub nadawców jak również treść wiadomości. Informacje można dodawać do wiadomości lub z nich usuwać, a sposób przekazywania wiadomości można modyfikować. Wiadomości można przysyłać dalej, kopiować, wysyłać do list dystrybucyjnych, odrzucać, opóźniać lub kierować ponownie do kolejki pocztowej.

Wszystkie te działania można łączyć w złożone reguły i wiązać z wypełnieniem konkretnych warunków.

ŁATWOŚĆ OBSŁUGI

Kwarantanna Użytkownika jest bardzo łatwa w obsłudze i nie wymaga zarządzania przez wykwalifikowaną osobę. Dostęp do kwarantanny użytkownika końcowego ma miejsce po podaniu jednorazowego hasła (generowanego przez tokena), podawanego w dziennych

raportach z kwarantanny. Mechanizm ten sprawia, że nie ma potrzeby używania nazw użytkownika i haseł, które tworzyć i przechowywać musiałby administrator. Nie ma również problemów ze zgubionymi hasłami. Użytkownicy mogą tworzyć swoje własne białe listy w oparciu o domeny lub adresy e-mail bezpośrednio z dziennego raportu, bez potrzeby uprzedniego logowania się do swojej kwarantanny.

Dzięki silnikowi heurystycznemu nie jest również konieczne informowanie MFILTRO o spamie. Oszczędza to użytkownikom czasu, jaki musieliby spędzić na klasyfikacji maili i odsyłaniu raportów do urządzenia.

NETASQ MFILTRO można w pełni skonfigurować przy pomocy 10-minutowego instalatora, obejmującego rejestrację, aktualizację firmware'u, konfigurację przesyłania wiadomości e-mail, wyjątki oraz ustawienia kwarantanny użytkownika. Dzięki temu administrator może praktycznie podłączyć urządzenie i o nim zapomnieć, jako że po instalacji zakres wymaganej obsługi jest minimalny.

Łatwość obsługi zarówno przez administratora jak i użytkowników maksymalnie skraca czas, jaki trzeba spędzić na konfiguracji i obsłudze urządzenia, co **gwarantuje najwyższy poziom zwrotu z inwestycji**.

WNIOSKI

Techniki opisane w niniejszym dokumencie czynią NETASQ MFILTRO jednym z **najskuteczniejszych** rozwiązań do walki ze spamem na dzisiejszym rynku. 10-minutowy instalator oraz nieskomplikowana kwarantanna użytkownika końcowego gwarantują **łatwość obsługi**.

NETASQ MFILTRO w walce ze spamem i wirusami korzysta z szeregu rozwiązań najwyższej klasy. Do walki z wirusami NETASQ MFILTRO używa skanera Clam AV oraz nagradzanego wielokrotnie rozwiązania antywirusowego dla bram internetowych firmy Kaspersky. Zaawansowany silnik heurystyczny zatrzymuje ataki wirusów i spamu jeszcze zanim dostępne są aktualizacje baz sygnatur.

O FIRMIE NETASQ

NETASQ specjalizuje się w rozwiązaniach do zintegrowanego zabezpieczenia sieci. Jako główny cel firma postawiła sobie dostarczanie rozwiązań zapewniających ten sam, najwyższy poziom zabezpieczeń dla firmy niezależnie od ich wielkości.

Rozwiązania NETASQ obecne są na rynkach w blisko 50 krajach poprzez sieć autoryzowanych partnerów również w Polsce.

Urządzenia NETASQ UTM posiadają m. in. certyfikację Common Criteria EAL4+ na kluczowe funkcje urządzeń czyli firewall, system wykrywania i blokowania włamań oraz VPN.