



Trend Micro™

Smart Protection Network

Powstrzymaj zagrożenia internetowe, zanim się z nimi zetkniesz. Inteligentniejsza forma ochrony.

Trend Micro Smart Protection Network to infrastruktura ochronna nowej generacji, działająca na treściach przesyłanych między internetem, a urządzeniami klienckimi użytkownika i chroniąca go przed płynącymi z internetu zagrożeniami. Dzięki połączeniu technologii opartych na rozwiązaniach internetowych z niewielkimi, lekkimi klientami, zyskujesz natychmiastowy dostęp do najnowszych zabezpieczeń, niezależnie od tego, czy łączysz się z internetem z domu, z sieci firmowej, czy w trakcie podróży. Oferujemy ci inteligentniejszą formę ochrony.

PROBLEM

Internet stał się potężną platformą, która zmieniła sposób prowadzenia interesów oraz sposób komunikacji. Zapewnia on anonimowość, dostęp do stale powiększającej się bazy użytkowników, ale jest także źródłem nowych technologii, które, rozwijając się, ujawniają coraz to nowe, łatwe do wykorzystania słabe strony. Za każdym razem, gdy przeglądamy witrynę internetową lub klikamy umieszczony w wiadomości e-mail adres URL, narażamy siebie i innych na pochodzące z internetu niebezpieczeństwo. Współczesne zagrożenia wiążą się z działaniem cyberprzestępców, motywowanych chęcią zysku i wykorzystujących rozwój Internetu do budowania swojej potężnej, podziemnej gospodarki.

Współczesne zagrożenia są skomplikowane i poważne. Zagrożenia internetowe to zwykle wielowarstwowe, skoordynowane ataki, prowadzące m.in. do znacznych strat finansowych, kradzieży tożsamości, utraty własności intelektualnej lub tajemnic handlowych. Gra toczy się nie tylko o informacje, ale również o reputację osób i firm.

Liczba złośliwych ataków rośnie wykładniczo. W 1988 roku firmy informatyczne zajmujące się zabezpieczeniami miały do czynienia z 1738 przykładami zagrożeń. Dla porównania, wystarczyły dwa pierwsze miesiące 2008 roku, aby zgłoszono ponad 1,1 miliona takich odrębnych przypadków. Od 2005 roku, firma Trend Micro odnotowała wzrost liczby zagrożeń internetowych o 1731%.

W odpowiedzi, dostawcy zabezpieczeń wprowadzają coraz częstsze aktualizacje sygnatur. Przytłaczający wzrost liczby zagrożeń oraz wynikająca z niego ogromna liczba wymaganych uaktualnień znacznie zwiększa obciążenie zasobów systemowych przeznaczonych do zarządzania pobieraniem sygnatur, a to z kolei prowadzi do poważnych problemów z wydajnością.

ROZWIĄZANIE

Rozwiązanie Trend Micro Smart Protection Network zapewnia ochronę w oparciu o koncepcję bardziej inteligentną, niż dotychczasowe, konwencjonalne podejścia. Polega ona na blokowaniu najnowszych zagrożeń jeszcze zanim zyskasz możliwość się z nimi bezpośrednio zetknąć.

Korzystająca z rozwiązań i usług firmy Trend Micro infrastruktura Trend Micro Smart Protection Network to połączenie unikalnych technologii internetowych i niewielkich klientów, z jednej strony skuteczniej Cię chroniąca, z drugiej — zmniejszająca Twoją zależność od czasochłonnego pobierania sygnatur.

Trend Micro Smart Protection Network to działający w czasie rzeczywistym mechanizm zabezpieczający, gromadzący dane z wielu źródeł, chroniący przed wszystkimi rodzajami zagrożeń: od złośliwego oprogramowania, spamu, phishingu i zagrożeń internetowych, po ataki typu DoS, luki w witrynach internetowych, a nawet utratę danych. Identyfikację niebezpieczeństw opiera on na kontroli jednoczesnego występowania różnego rodzaju czynników, co pozwala mu określić, czy mają one złośliwy charakter. Pojedyncze zagrożenie internetowe może bowiem wydawać się niegroźne, lecz w połączeniu z kilkoma innymi może wyrządzić poważne szkody.

Powstrzymaj zagrożenia internetowe, zanim się z nimi zetkniesz. Sięgnij po inteligentniejszą formę ochrony.

NAJWAŻNIEJSZE KOMPONENTY

- Technologia Web Reputation
- Technologia Email Reputation
- Technologia File Reputation
- Korelacja z analizą zachowań
- Pętle informacji zwrotnych
- Pozyskiwanie informacji o zagrożeniach (gromadzenie i analiza zagrożeń)

GŁÓWNE KORZYŚCI

- Nowe zagrożenia, nowa forma ochrony
- Skuteczniejsza i szybsza ochrona — mniejsze obciążenie zasobów systemowych
- Ochrona zawsze i wszędzie
- Ochrona wielowarstwowa
- Ochrona kompleksowa
- Ochrona typu „lepiej razem”
- Wsparcie i wiedza liderów z dziedziny ochrony treści

NAJWAŻNIEJSZE KOMPONENTY

Technologia Web Reputation

Technologia Web Reputation korzysta z jednej z największych na świecie baz danych reputacji domen, co pozwala określać wiarygodność konkretnych domen sieci Web na podstawie przyznawanej im oceny punktowej, ustalonej w oparciu o takie czynniki, jak wiek witryny, historyczne zmiany lokalizacji oraz ślady podejrzanych działań odkryte za pomocą analizy złośliwego zachowania.

Technologia Email Reputation

Technologia Email Reputation firmy Trend Micro sprawdza adresy IP pod kątem ich obecności w bazie znanych źródeł spamu oraz przy użyciu dynamicznej usługi, będącej w stanie ocenić reputację nadawcy poczty elektronicznej w czasie rzeczywistym. Oceny reputacji są bardzo precyzyjne, a to dzięki ciągłej analizie „zachowań” adresów IP, zakresu związanych z nimi działań i ich historii. Złośliwe wiadomości e-mail są blokowane jeszcze po stronie internetu w oparciu o adres IP nadawcy, nie docierając tym samym w ogóle do sieci lub komputera użytkownika.

Technologia File Reputation

Wykorzystywana w otoczeniu sieciowym technologia File Reputation sprawdza w rozbudowanej bazie danych reputację każdego pliku umieszczonego w witrynie internetowej lub dołączonego do wiadomości e-mail. Dopiero po przejściu takiej kontroli system umożliwia użytkownikowi do niego dostęp. Dzięki dużej przepustowości sieci dostarczających treść oraz zastosowaniu lokalnych serwerów buforujących, czasy opóźnień redukowane są do minimum. Informacje o złośliwym oprogramowaniu są przechowywane w internecie, dzięki czemu są bezpośrednio dostępne dla wszystkich użytkowników chronionej sieci.

Korelacja z analizą zachowań

Technika korelacji z analizą zachowań pozwala sprawdzać współwystępowanie różnego rodzaju aktywności w celu określenia, czy w połączeniu ze sobą mają one złośliwy charakter. Pojedyncze zagrożenie internetowe może bowiem wydawać się niegroźne, lecz w połączeniu z kilkoma innymi może spowodować fatalne skutki. Dzięki sprawdzaniu współzależności między różnymi składnikami zagrożeń i ciągłej aktualizacji baz danych zagrożeń, firma Trend Micro zyskała niezaprzeczalny atut, jakim jest zdolność udzielania odpowiedzi w czasie rzeczywistym oraz możliwość zapewnienia natychmiastowej i automatycznej ochrony przed zagrożeniami związanymi z korzystaniem z sieci WWW i poczty elektronicznej.

Pętla informacji zwrotnych

Zintegrowane pętla informacji zwrotnych zapewniają ciągłą komunikację między produktami firmy Trend Micro a jej działającymi non stop ośrodkami badawczymi i zasobami technicznymi. Każde nowe zagrożenie, zidentyfikowane przez rutynową kontrolę reputacji przeprowadzoną u pojedynczego użytkownika, automatycznie aktualizuje wszystkie bazy danych zagrożeń firmy Trend Micro, co powoduje blokadę wszystkich jego przyszłych wystąpień. Gromadzone informacje o zagrożeniach opierają się na reputacji źródła komunikacji, z którego ono pochodzi, a nie na treści komunikacji, dlatego zawsze zachowana jest poufność osobistych lub firmowych danych użytkownika.

Pozyskiwanie informacji o zagrożeniach

Firma Trend Micro, od 20 lat lider w dziedzinie bezpieczeństwa pochodzących z Internetu treści, posiada w pięciu miejscach na świecie centra danych, przetwarzające codziennie ponad 1,2 terabajta danych. Globalna sieć ośrodków firmy Trend Micro zajmujących się badaniami, obsługą i pomocą techniczną — TrendLabs™ — zaangażowana jest w ciągłe rozpoznawanie zagrożeń i ochronę przed atakami. Dysponując ponad 1000 specjalistów z dziedziny zabezpieczeń i działających przez 24 godziny na dobę, 7 dni w tygodniu, zespół TrendLabs opracowuje mechanizmy wykrywania ataków, zapobiegania im oraz eliminowania ich w czasie rzeczywistym.

Infrastruktura Trend Micro Smart Protection Network w sposób ciągły przetwarza pozyskiwane dane o zagrożeniach. Pochodzą one z rozległej sieci pułapek typu honeypot, pętli zwrotnych, robotów przeglądających sieć WWW, a także bezpośrednio od użytkowników, partnerów oraz zespołu TrendLabs. W rezultacie użytkownicy rozwiązania mogą korzystać z automatycznej ochrony w czasie rzeczywistym, skutecznej także przeciwko najnowszym zagrożeniom. Zgromadzone dane o zagrożeniach są analizowane i sprawdzane w czasie rzeczywistym za pomocą zapytań do baz danych wiedzy o złośliwym oprogramowaniu oraz przez laboratoria TrendLabs.

Więcej informacji można znaleźć pod adresem <http://www.trendmicro.com/go/SmartProtectionNetwork>.



• Copyright© 2008 Trend Micro Incorporated. Wszelkie prawa zastrzeżone. Trend Micro, logo t-ball firmy Trend Micro oraz TrendLabs są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Trend Micro Incorporated. Pozostałe nazwy firm i produktów mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi odpowiednich właścicieli. [DS01SPN_080804PL]

KILKA LICZB

- Infrastruktura Trend Micro Smart Protection Network przetwarza dziennie ponad pięć miliardów zapytań dotyczących adresów URL, adresów poczty elektronicznej i plików.
- Firma Trend Micro przetwarza ponad 50 milionów adresów IP i URL dziennie.
- Ponad 250 milionów próbek trafia do analizy z globalnego systemu gromadzenia zagrożeń firmy Trend Micro, obejmującego pułapki typu honeypot, informacje zwrotne przesyłane przez produkty oraz inne sprawdzone techniki gromadzenia wiedzy.
- Firma Trend Micro posiada ośrodki przetwarzania danych w pięciu różnych miejscach na świecie, łącznie przetwarzając dziennie ponad 1,2 terabajta danych.
- Firma Trend Micro zatrudnia ponad 1000 specjalistów z dziedziny zabezpieczeń, którzy pracują nad rozpoznawaniem zagrożeń i ochroną przed atakami.
- Każdego dnia firma Trend Micro zapobiega 8–10 milionom infekcji.