Technologie TruPrevent

Dokonalá ochrana proti virům bez aktualizací

Klasické antivirové programy už brzy dosloužíí. Největší šance v boji proti útokům z internetu dávají odborníci novým technologiím typu TruPrevent. Ty totiž poznají viry a červy podle profilu pachatele, nikoli podle otisku prstů.

Text: Valentin Pletzer, *autor@chip.cz*

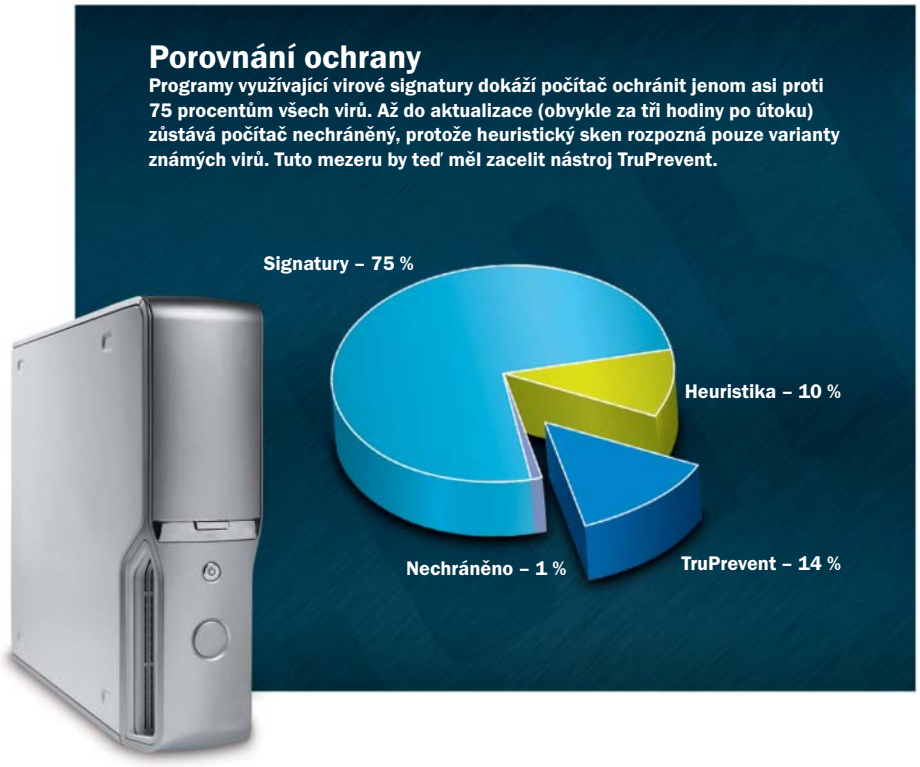
Výhodu nové technologie pro boj proti počítačovým virům popisuje José María Hernández, viceprezident společnosti Panda Software pro mezinárodní expanzi, jednoduše: má před viry náskok. Pod názvem TruPrevent nabízí španělská firma novou zbraň v boji proti internetové mafii a programátorům virů. Nové je na ní to, že její technologie ochrany pracuje s propracovanými profily útočníků, které místo odhalování škůdců podle otisků prstů analyzují jejich chování. Program TruPrevent je koncipován jako doplněk k běžným antivirovým programům a měl by uzavřít mezeru v bezpečnostním systému počítače až do doby, než výrobce antivirového programu uveřejní aktuální signatury.

Zatím to totiž funguje tak, že výrobce antivirového programu může na nový virus reagovat až v okamžiku, kdy takový virus napadne počítač a zanechá po sobě otisk. Teprve potom může nabídnout protilék. Proto většina firem zabývajících se bezpečností pracuje intenzivně na tom, jak výrazně zkrátit dobu reakce mezi výskytem viru a vytvořením signatury. Nové varianty už známých virů by měl pomáhat odhalovat heuristický sken. Obě metody ale mají svá slabá místa. Škodlivé kódy, jako např. červ Witty, se dokážou rozšířit během pár hodin, a tak výrobci nejsou schopni zveřejňovat nové signatury včas. Heuristický sken zase neodhalí úplně nové škůdce.

Klasické antivirové programy navíc uživatele obtěžují falešnými poplachy. Často se například stává, že antivirový program identifikuje antispyware jako virus, a to jenom proto, že tento užitečný nástroj spravuje databázi známých virových signatur.

TruPrevent blokuje viry i bez signatury

Řešení přichází z oblasti podnikových sítí. Ve snaze ochránit je před hackery byly už před mnoha lety vyvinuty tzv. systémy prevence proti průniku (intrusion prevention systems). Tyto nástroje zapisují do protokolu veškeré údaje o provozu v síti a hlásí podezřelé aktivity. TruPrevent funguje podobně. Program sleduje chování všech procesů, které v počítači právě běží. Pokud některou aplikaci vyhodnotí jako nebezpečnou, ukončí ji a propříště ji zablokuje.
O tom, že to skutečně funguje, jsme se přesvědčili v testu, který prováděl nezávislý expert na počítačové viry Andreas Marx z firmy AV-Test. TruPrevent odhalil a zablokoval známé červy Sobig a Blaster i bez příslušných signatur.

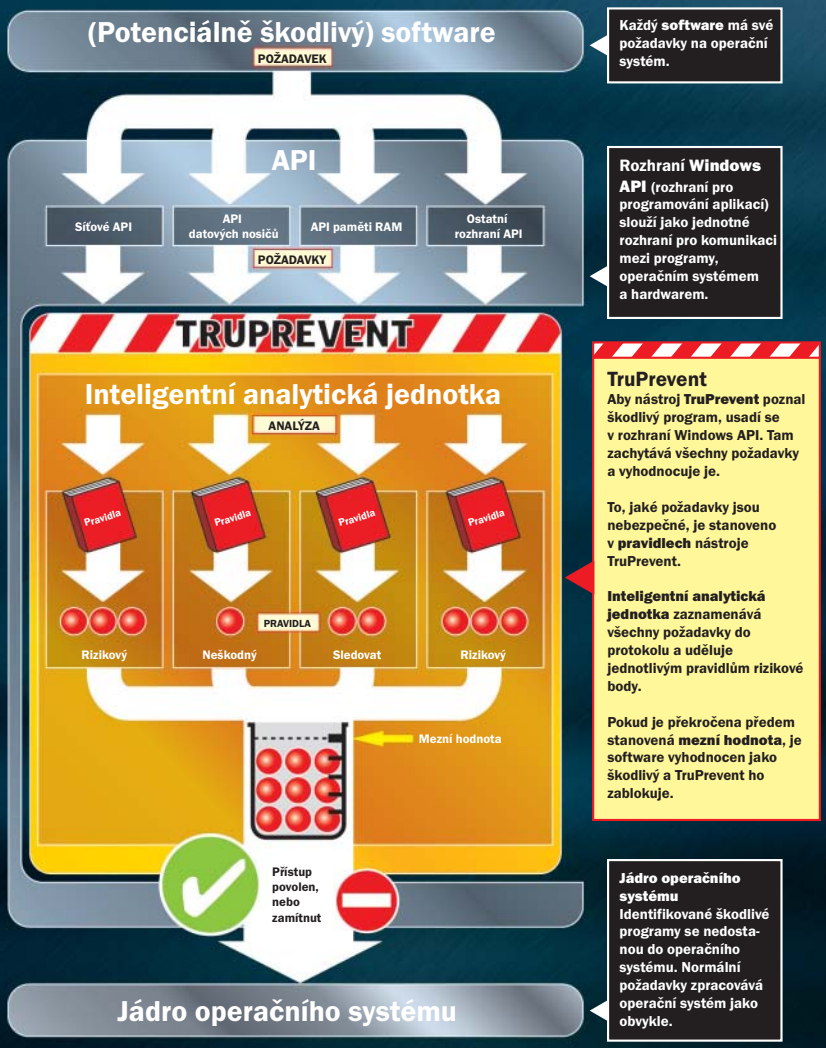


Odposlouchávání útočníků

Aby mohl TruPrevent sledovat programy spuštěné pod Windows, usazuje se podobně jako rootkit přímo do operačního systému. Nejlepším místem je API (rozhraní pro programování aplikací). Ve Windows totiž programy nekomunikují s hardwarem přímo, nýbrž předávají své příkazy operačnímu systému právě prostřednictvím rozhraní API. Operační systém pak zajišťuje koordinaci jednotlivých procesů, vybírá správný ovladač a provádí příkaz.

TruPrevent zasahuje do tohoto procesu. Sleduje každou komunikaci s rozhraním API a zaznamenává ji do protokolu. Potom svůj protokol porovnává se souborem záznamů vytvořeným firmou Panda Software a odhaduje nebezpečnost procesů. Jakmile se nějaký program pokusí porušit důležité pravidlo, TruPrevent ho okamžitě zablokuje. Porušení méně důležitého pravidla nejprve jenom zaznamená do protokolu a přiřadí mu bodové hodnocení.

Jak funguje TruPrevent



Inteligentní analýza odhaluje hackery a zloděje hesel

Aby mohl program otevřít nějaký soubor na pevném disku, musí ke čtení a zapisování na datový nosič využít rozhraní Windows API. TruPrevent se tak dozví, jaký soubor chce program otevřít. Jestliže tedy program hodlá například spustit soubor EXE, který patří aplikaci Adobe Reader, a tento soubor pak změnit nebo nahradit, může to být signálem nechtěného procesu. Je možné, že se nějaký virus pokouší přidat k programu svůj škodlivý kód, aby se mohl rozmnožovat. Může se ale také jednat o zcela neškodnou aktualizaci od výrobce programu, který se tak snaží nahradit soubor EXE novou, opravenou verzí.

Takový proces pak TruPrevent ohodnotí vysokým počtem rizikových bodů, ale neukončí ho hned. Místo toho ho sleduje a provádí další hodnocení. Teprve až celkový počet bodů překročí mezní hodnotu stanovenou firmou Panda Software, označí program za potenciálně nebezpečný a zabrání jeho spuštění.

TruPrevent sleduje rozhraní API nejen jednotlivých datových nosičů, ale i sítě a paměti RAM. Jakmile se například nějaký program pokusí během velmi krátké doby navázat spojení s velkým počtem různých portů, může to být první signál útoku zvenčí. Pokus proniknout do paměti jiných aplikací zase může ukazovat na zloděje hesel.

Zvláštností programu TruPrevent je inteligentní analýza protokolu API. Bodová hodnocení jednotlivých přístupů k rozhraní API se vzájemně porovnávají a vyhodnocují. Pokud je překročena mezní hodnota, TruPrevent proces označený jako škodlivý ukončí a zabrání jeho dalšímu spouštění.

V některých případech je škodlivý program zastaven okamžitě. Inteligentní analýza totiž neustále sleduje všechna pravidla a přístup k rozhraní API ihned ukončí, pokud dojde k jejich zřejmému porušení, například když se nějaká aplikace snaží změnit soubor INI nebo do něj zapisovat. Mohlo by se totiž jednat o pokus hackera proniknout do systému.

Správci systémů ale musí čas od času soubory INI otvírat a prohlížet si jejich obsah v Poznámkovém bloku Windows. TruPrevent proto nebrání spuštění textového editoru, ale až snaze změnit soubor INI nebo do něj zapisovat. Správcům systému navíc firma Panda Software nabízí profesionální verzi nástroje TruPrevent, která umožňuje definovat vlastní pravidla, tedy například povolit oprávněné změny v souborech INI.

Protože nástroj TruPrevent každý přístup programů přes rozhraní operačního systému nejen odposlouchává, ale také ihned analyzuje a zaznamenává do protokolu, platí uživatel za tento typ ochrany vysokou cenu v podobě nároků na paměť RAM a především výpočetní výkon. Ještě že mají nové 64bitové procesory a systémy s dvěma jádry dostatečný výkon na to, aby mohly být programy typu TruPrevent neustále spuštěné.

Dalším problémem je opožděná reakce. TruPrevent sice chrání mnohem rychleji než běžné aktualizace signatur, ale aby mohl program posoudit, musí mu nejdřív povolit přístup k rozhraní API. Škodlivý kód tak v nejhorším případě může napáchat škodu, ještě než jeho počet bodů překročí kritickou mez.

Krok správným směrem, další výrobci se přidávají

S novou technologií TruPrevent se firma Panda Software vydává správnou cestou. Protože je stále více počítačů propojováno do sítí a toto propojení je stále rychlejší, zvětšuje se také neustále časový odstup mezi programátory virů a antivirovými firmami – bohužel v neprospěch těch druhých. Díky nástroji TruPrevent se ale náskok útočníků zatím aspoň výrazně zkracuje.

Uvědomují si to i další výrobci, jako Kaspersky Labs, Symantec a McAfee. Podobnou technologií ochrany zřejmě vybaví už příští verzi svých programů. Chtějí je také rozšířit o funkci rollback, která by uživatelům umožňovala vrátit zpátky všechny operace provedené škodlivým programem. Zdá se, že bez takovýchto ochranných mechanismů se v budoucnu na trhu neudrží žádný balík bezpečnostních aplikací. ■ ■ ■