Előszó

Kinek szól a könyv?

Az elmúlt két évtizedben több írás jelent meg a számítógépes vírusokról, ám csupán néhány tanulmányt készítettek a számítógépes vírusok kutatásában jártas szakemberek (a „bennfentesek"). Több könyv látott napvilágot, amely a számítógépes vírusok problémakörét tárgyalja, ezek azonban rendszerint az érdeklődő közönségnek szólnak, nem pedig szakemberek számára készültek. Csak néhány munka nyújt kellő mélységű összefoglalást a technikai részletekről ahhoz, hogy a számítógépes vírusok elleni hatékony védelmet ki lehessen alakítani.

Az egyik probléma az, hogy a forgalomban lévő könyvek kevés információt tartalmaznak (ha tartalmaznak egyáltalán) a számítógépes vírusok aktuális komplexitásáról. Hiányos technikai információkkal rendelkeznek például azokról a rendkívül kártékony számítógépes férgekről, amelyek kihasználják a biztonsági réseket, és betörnek a célrendszerekbe; vagy nem tesznek említést a legújabb kódevolúciós módszerekről, például a kódmetamorfizmusról. Ha valaki szeretné mindazt az információt megszerezni, amelyet ebben a könyvben összegeztem, rengeteg időt kellene cikkek és tanulmányok böngészésével töltenie, amelyek gyakran a számítógépes vírusokkal és a biztonsággal kapcsolatos konferenciák anyagaiban rejtőznek, és évekig kutathatná a rosszindulatú kódokat a megfelelő információk kinyeréséhez.

Hiszek abban, hogy a könyv rendkívül hasznos lesz azoknak a számítástechnikai szakembereknek, akik napi munkájuk során folytatnak küzdelmet a számítógépes vírusok ellen. Napjainkban mind a rendszergazdáknak, mind az otthoni felhasználóknak számítógépes férgekkel és egyéb rosszindulatú kódokkal kell elbánniuk a hálózatokon. A biztonsági tanfolyamok sajnos igen kevés anyaggal szolgálnak a számítógépes vírusvédelemről, és az átlagos felhasználók nagyon keveset tudnak arról, hogyan elemezzék és védjék meg a hálózatokat az efféle támadásoktól. Tovább nehezíti a dolgot, hogy a számítógépes vírusok elemzésének módszereit egyetlen korábbi munka sem tárgyalta kellő részletességgel.

Úgy vélem, hogy bárkinek, akit érdekel az információs biztonság, fontos tisztában lennie azzal, hogy a számítógépes vírusok készítői milyen eredményeket „értek el" eddig.

Hosszú évekig a számítógépes vírusok kutatói fájlokra és fertőzött objektumokra összpontosítottak. Ezzel szemben a biztonságtechnikai szakembereket a hálózati szintű gyanús események érdekelték, továbbá az olyan fenyegetések, mint a CodeRed féreg, amely a hálózaton a sérülékeny folyamatok me-

móriájába ágyazta magát, de a lemezen egyetlen objektumot sem fertőzött meg. Elengedhetetlenül fontos ezeknek a főbb perspektíváknak a megértése – a fájlok (a tárolóegységen), a memóriában előidézhető károk és a hálózati nézetek ismerete –, és ezeket összefüggésbe kell hoznunk a rosszindulatú kódok elemzési módszereivel.

Az évek során nagyon sok számítógépvírus- és biztonságelemzőt oktattam a rosszindulatú kódfenyegetések hatékony elemzésére és kezelésére. A könyvben minden olyan információt összegyűjtöttem, amellyel valaha dolgom akadt. Régi fenyegetések példáival is szolgálok, például a Commodore 64-es számítógépek 8 bites vírusaival. Kiderül majd, hogy az olyan technológiák, mint a lopakodó technológia a legelső számítógépes vírusokban, több platformon is megjelent. Így pedig beláthatjuk, hogy a legújabb rootkitek tulajdonképpen nem is képviselnek semmi újat. Részletes elemzést találunk a 32 bites Windows-féreg-fenyegetésekről, valamint a 64 bites vírusokról és a mobileszközök „zsebszörnyetegeiről". Az volt a célom, hogy bemutassam, a régi módszerek hogyan „reinkarnálódnak" új fenyegetések formájában, és kellő mennyiségű technikai részlettel illusztráljam a modern támadásokat.

Biztos vagyok benne, hogy sokan szeretnék felvenni a harcot a rosszindulatú kódok ellen, és talán hozzám hasonlóan többen újabb védelmi módszerek feltalálói lesznek. Ám mindenkinek tisztában kell lennie ennek a szakterületnek a csapdáival és a kihívásaival is.

Erről szól a könyv.

A könyv témaköre

A könyv célja, hogy bemutassa a számítógépes vírusok és a vírusvédelmi fejlesztések aktuális állapotát, valamint megismertesse a számítógépesvírus-elemzés és a vírusvédelem módszertanát. Az összes lehetséges szempontból megvizsgáljuk a számítógépes vírusok fertőzési módszereit: a fájlok (a tárolóegységen), a memória és a hálózat fertőzéseit. Csoportosítjuk és tanulmányozzuk a támadók által az utóbbi két évtizedben kifejlesztett számítógépes vírusok különböző trükkjeit, és megvizsgáljuk, hogyan lehet az olyan összetett problémákat kezelni, mint a polimorfizmus és a kihasználóvírusok.

A könyvet nyilvánvalóan fejezetről fejezetre haladva érdemes olvasni. Néhány, a támadásokról szóló fejezet azonban a védekezési fejezetekben tárgyalt módszerek megismerését követően nyer értelmet. Ha bármelyik fejezet túl bonyolultnak vagy hosszadalmasnak tűnik, bármikor a következő fejezetre lehet ugrani. Nyilvánvaló, hogy a személyes tapasztalatoktól függően lesz olyan, aki néhány részt nehéznek vél, más részeket pedig egyszerűnek talál.

Célszerű, ha az olvasó rendelkezik némi technológiai ismerettel és bizonyos programozási képességekkel. Túl sok dologról esik szó ahhoz, hogy minden témát teljes részletességgel meg lehessen vizsgálni. Ám a könyv arra rá-

világít, hogy milyen témakörökben kell elmélyedni ahhoz, hogy teljes sikerrel lehessen kivédeni a rosszindulatú támadásokat. Az olvasó dolgát megkönnyíti a fejezetekben található referencialista, amely a szükséges háttér-információkra mutat rá.

Ami a könyv témakörén túlmutat

Nem foglalkoztam részletesen a trójaifaló-vírusokkal vagy a hátsó ajtót nyitó vírusokkal. A könyv elsősorban az önmagát megsokszorozó, rosszindulatú kódokról szól. Nagyon sok könyv született a hagyományos rosszindulatú programokról, de nem ez a helyzet a számítógépes vírusokkal kapcsolatban.

A könyvben nem található egyetlen olyan víruskód sem, amellyel közvetlenül másik vírus készíthető. A könyv nem „vírusíró" tananyag. Véleményem szerint azonban a támadók már ismerik azokat a módszereket, amelyeket ebben a könyvben megvizsgálok. A védekezéssel foglalkozóknak viszont többet kell még tanulniuk, és úgy kell gondolkodniuk (de nem úgy cselekedniük), mint egy igazi támadónak, így fejleszthetik ki védelmi állásaikat.

Több egyetemen is próbálkoznak a számítógépes vírusok oktatásával: víruskészítési tárgyakat tartanak a hallgatóknak. Valóban jó ötlet megtanítani a diákokat olyan vírusok készítésére, amelyek világszerte számítógépek millióit fertőzhetik meg? Ettől jobban fogják tudni ezek a hallgatók, hogy hogyan fejlesszenek hatékonyabb védelmi technológiákat? A válasz nyilvánvalóan nem.

A tananyagnak a már létező rosszindulatú fenyegetésekre kellene összpontosítania. Nagyon sok fenyegetés létezik, ezeket meg kell érteni – és valamit tenni ellenük.

A számítógépképes vírusok ismerete olyan, mint a Csillagok háborújában az a bizonyos „Erő". A használójától függően a tudás a jó vagy a gonosz forrása lehet. Nem kényszeríthetünk senkit arra, hogy tartsa magát távol a „Sötét oldaltól", de melegen ajánlom.