December 2012

IMPERVA®

Hacker Intelligence Initiative, Monthly Trend Report #14

Assessing the Effectiveness of Antivirus Solutions

Executive Summary

In 2012, Imperva, with a group of students from The Technion – Israeli Institute of Technology, conducted a study of more than 80 malware samples to assess the effectiveness of antivirus software. Based on our review, we believe:

1. ***The initial detection rate of a newly created virus is less than 5%****. Although vendors try to update their detection mechanisms, the initial detection rate of new viruses is nearly zero. We believe that the majority of antivirus products on the market can't keep up with the rate of virus propagation on the Internet.*
2. ***For certain antivirus vendors, it may take up to four weeks to detect a new virus from the time of the initial scan****.*
3. ***The vendors with the best detection capabilities include those with free antivirus packages, Avast and Emsisoft****, though they do have a high false positive rate.*

These findings have several ramifications:

1. ***Enterprises and consumers spend on antivirus is not proportional to its effectiveness****. In 2011, Gartner reported that consumers spent $4.5 billion on antivirus, while enterprises spent $2.9 billion, a total of $7.4 billion. This represents more than a third of the total of $17.7 billion spent on security software. We believe both consumers and enterprises should look into freeware as well as new security models for protection.*
2. ***Compliance mandates requiring antivirus should ease up on this obligation****. One reason why security budgets devote too much money to antivirus is compliance. Easing the need for AV could free up money for more effective security measures.*
3. ***Security teams should focus more on identifying aberrant behavior to detect infection****. Though we don't recommend removing antivirus altogether, a bigger portion of the security focus should leverage technologies that detect abnormal behavior such as unusually fast access speeds or large volume of downloads.*

To be clear, we don't recommend eliminating antivirus.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Table of Contents

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Introduction and Motivation

Over the years and as the result of technological developments, the importance of personal computers in our lives has grown significantly. This has resulted in a desire by some to develop malicious applications, whether lone teenagers or nation states, and distribute them across the Internet where they attack a range of computer systems. As a result, the importance of antivirus software has grown significantly and has resulted in increasing demand for dependable antivirus products that can defend against the range of malicious viruses.

Anti-virus programs are meant to locate computer viruses and protect computers from their actions. Currently, antivirus software is considered a reliable and effective defense against viruses and in protecting computers. According to Gartner, enterprises and consumers spent $7.4 billion on antivirus in 2011 – a five-fold increase from 2002.[1] Antivirus, by contrast, has not seen a fivefold increase in effectiveness.

Every day, viruses and malicious programs are created and distributed across the Internet. In order to guarantee effectiveness and maximum protection, antivirus software must be continuously updated. This is no small undertaking when taking into consideration the fact that computers connected to the Internet are exposed to viruses from every direction and delivered using any range of methods: Infected servers and files, USB drives, and more. Viruses involuntarily draft consumers into bot armies while employees can become unknowing compromised insiders helping foreign governments or competitors.

Background

In 1988, 'Antivir' was the first antivirus product that came to market and was meant to protect against more than a single virus. The age of the Internet had brought about the proliferation of viruses, their method of infection, and means of distribution. Subsequently, antivirus companies were forced to combat this threat. They began to release new versions of their products at a much faster rate and began to update the signature database of their products via the Internet.

In today's market, there is a wide variety of antivirus products, some that are freeware, and others that cost money. Studies show that the majority of people prefer and settle for freeware antivirus. Furthermore, the popularity of any given antivirus product does not reflect its effectiveness. The below diagram illustrates the popularly of the major antivirus products with the largest market share. Though as noted, the percentages in this diagram do not necessarily reflect given products capabilities.

According to one study, here are the most popular antivirus products:[2]

- Avast - 17.4% worldwide market share
- Microsoft - 13.2% worldwide market share
- ESET - 11.1% worldwide market share
- Symantec - 10.3% worldwide market share
- AVG - 10.1% worldwide market share
- Avira - 9.6% worldwide market share
- Kaspersky - 6.7% worldwide market share
- McAfee - 4.9% worldwide market share
- Panda - 2.9% worldwide market share
- Trend Micro - 2.8% worldwide market share
- Other - 11.1% worldwide market share

[1] Gartner, *Worldwide Spending on Security by Technology Segment, Country and Region*, 2010-2016 and 2002
[2] http://www.zdnet.com/blog/security/which-is-the-most-popular-antivirus-software/12608

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Locating and Collecting Viruses

The purpose of this work was to evaluate AV software's ability to detect previously non-cataloged malware samples. Hence, we could not rely on any of the existing malware databases. We therefore resorted to other means of virus hunting over the Web. We have employed various methods for collecting malware samples as described below. We executed the samples in a controlled environment to make sure that they display behavior indicative of malware. Using the methods described below, we were able to collect 82 samples.

Honey Pots

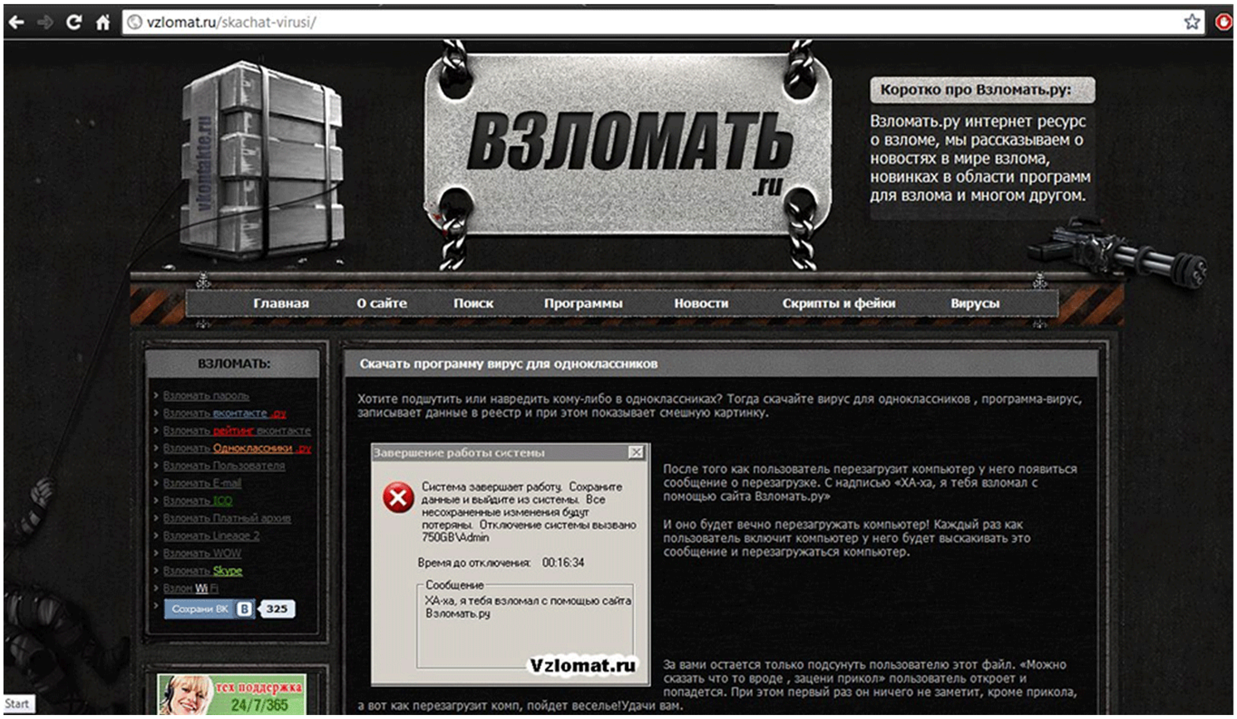
We have a number of Web honey pots deployed over the Web. Through these servers, we were able to detect access by hackers to Web repositories where they deposit the malware they have acquired. We then visited these repositories and were able to obtain the deposited files.

Google Search

We searched Google for specific patterns that yield references to small malware repositories. We then accessed these repositories to obtain samples. We used distinguishable file names we have seen through our honey pot (see above) to successfully find and collect more samples. Names like `1.exe` or `add-credit-facebook1.exe` yielded good results.

Hacker Forums

We looked through hacker forums for references to copies of malware. Focus was Russian language forums such as the one below:



Коротко про Взломать.ру:

Взломать.ру интернет ресурс о взломе, мы рассказываем о новостях в мире взлома, новинках в области программ для взлома и многом другом.

Скачать программу вирус для одноклассников

Хотите подшутить или навредить кому-либо в одноклассниках? Тогда скачайте вирус для одноклассников , программа-вирус, записывает данные в реестр и при этом показывает смешную картинку.

Завершение работы системы

Система завершает работу. Сохраните данные и выйдите из системы. Все несохраненные изменения будут потеряны. Отключение системы вызвано 750GB\Admin

Время до отключения: 00:16:34

Сообщение

ХА-ха, я тебя взломал с помощью сайта Взломать.ру

После того как пользователь перезагрузит компьютер у него появиться сообщение о перезагрузке. С надписью «ХА-ха, я тебя взломал с помощью сайта Взломать.ру»

И оно будет вечно перезагружать компьютер! Каждый раз как пользователь включит компьютер у него будет выскакивать это сообщение и перезагружаться компьютер.

За вами остается только подсунуть пользователю этот файл. «Можно сказать что то вроде , зацени прикол» пользователь откроет и попадется. При этом первый раз он ничего не заметит, кроме прикола, а вот как перезагрузит комп, пойдет веселье!Удачи вам.

The screenshot displays one of the websites that we found effective. In the menu on its left-hand side, users can obtain the following malicious software:

› Program for hacking ICQ

› Program for hacking e-mail

› Program for hacking Skype

› Program for hacking accounts on Odnoklassniki and vkontakte (Russian Social Networks)

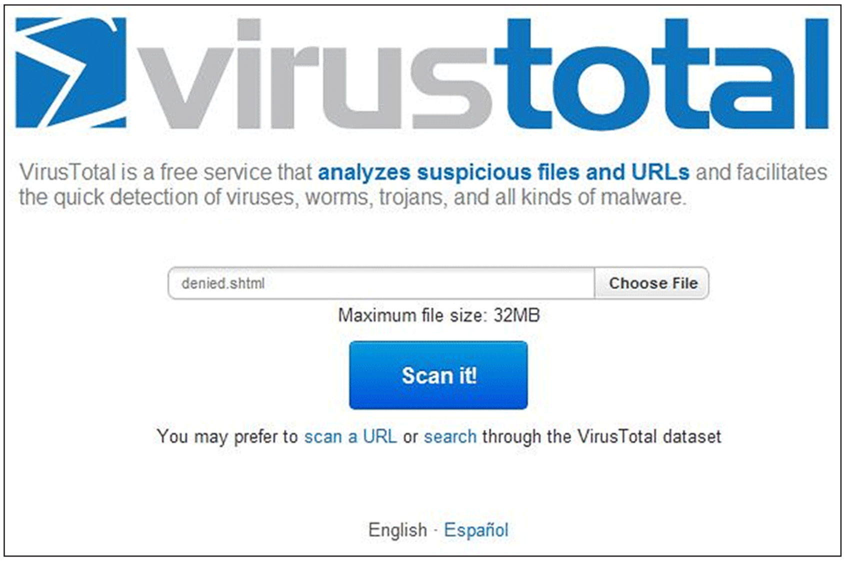
DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

Evaluating the Samples Against Antivirus Products

Now that we had 82 malware samples, we needed an infrastructure that would allow us to evaluate them with as many AV products as possible, repeatedly over time.

VirusTotal (www.virustotal.com) is a website that provides a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans, and other kinds of malicious content detected by antivirus engines and website scanners. At the time of our work, each sample was tested by 40 different products. A detailed report is produced for each analysis indicating, for each AV product, whether the sample was identified as malware, and if so, which malware was detected. The following figures show sample screenshots of a manual evaluation process (in which a user uploads the malware sample through a browser and reviews results in HTML form).

VirusTotal File Upload Page

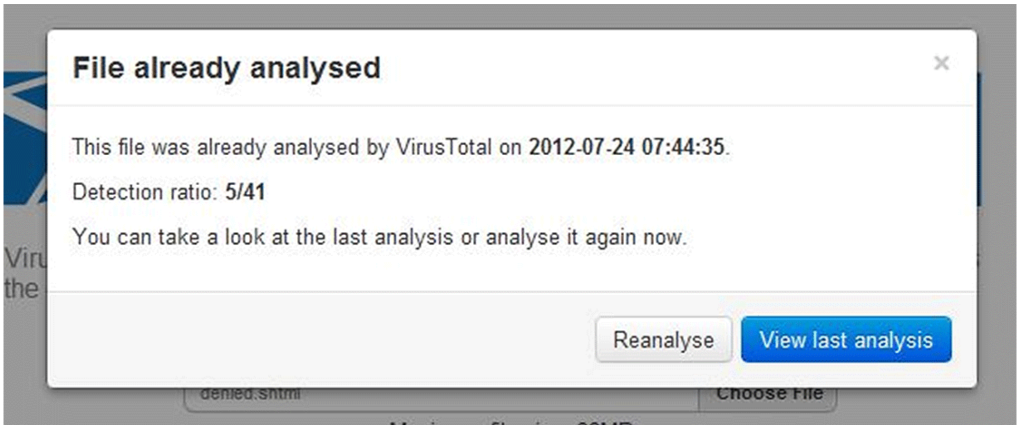


VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Maximum file size: 32MB

You may prefer to scan a URL or search through the VirusTotal dataset

Last Scan Results



File already analysed

This file was already analysed by VirusTotal on **2012-07-24 07:44:35**.

Detection ratio: **5/41**

You can take a look at the last analysis or analyse it again now.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE