

## 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.*

## Table of Contents

<b>Executive Summary</b>	<b>1</b>
<b>Introduction and Motivation</b>	<b>3</b>
<b>Background</b>	<b>3</b>
<b>Locating and Collecting Viruses</b>	<b>4</b>
Honey Pots	4
Google Search	4
Hacker Forums	4
<b>Evaluating the Samples Against Antivirus Products</b>	<b>5</b>
<b>Analyzing the Results</b>	<b>7</b>
General Statistics	7
Specific Samples	10
<i>Fake Google Chrome Installer</i>	10
<i>Multipurpose Trojan with Fake AV</i>	11
<b>Conclusion</b>	<b>12</b>
<b>Limitations, Objections and Methodology</b>	<b>12</b>
<b>References</b>	<b>13</b>

## 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.<sup>1</sup> 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 popularity 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:<sup>2</sup>

- › 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

<sup>1</sup> Gartner, *Worldwide Spending on Security by Technology Segment, Country and Region*, 2010-2016 and 2002

<sup>2</sup> <http://www.zdnet.com/blog/security/which-is-the-most-popular-antivirus-software/12608>

## 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

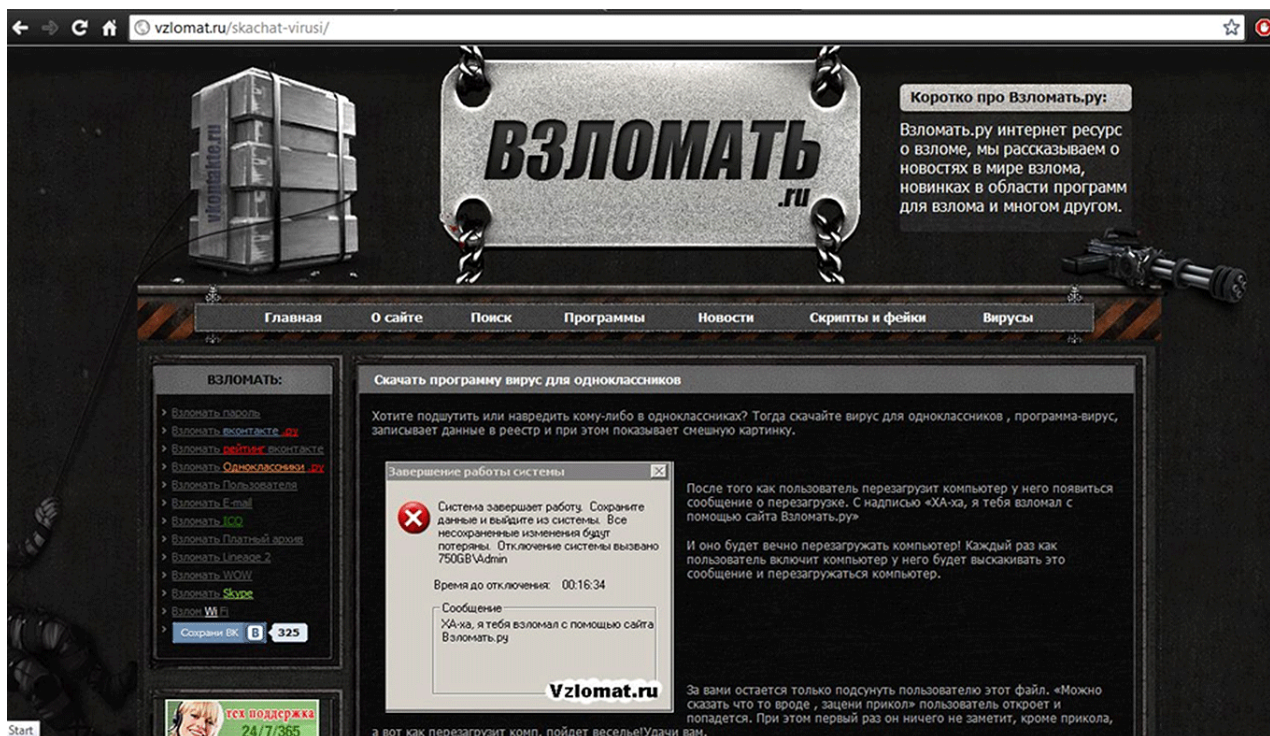
We have a number of Web honey pots deployed over the Web. Through these servers, we were able to detect access by hackers to Web repositories where they deposit the malware they have acquired. We then visited these repositories and were able to obtain the deposited files.

### 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:



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)

## 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.

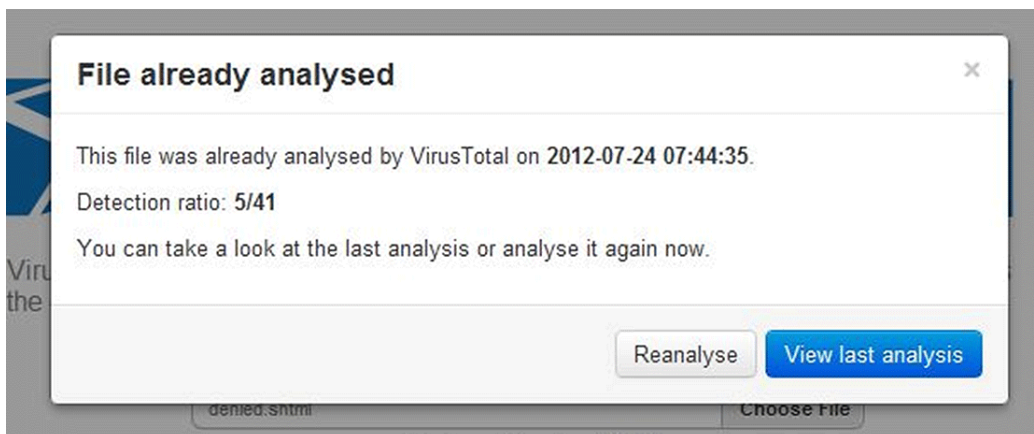
VirusTotal ([www.virustotal.com](http://www.virustotal.com)) is a website that provides a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans, and other kinds of malicious content detected by antivirus engines and website scanners. At the time of our 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



The screenshot shows the VirusTotal file upload interface. At the top is the VirusTotal logo. Below it is a description: "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." There is a text input field containing "denied.shtml" and a "Choose File" button. Below the input field, it says "Maximum file size: 32MB". A large blue "Scan it!" button is centered. Below the button, it says "You may prefer to scan a URL or search through the VirusTotal dataset". At the bottom, there is a language selector: "English - Español".

### Last Scan Results



The screenshot shows a dialog box titled "File already analysed" with a close button (X) in the top right corner. The text inside the dialog reads: "This file was already analysed by VirusTotal on 2012-07-24 07:44:35." followed by "Detection ratio: 5/41" and "You can take a look at the last analysis or analyse it again now." At the bottom of the dialog, there are two buttons: "Reanalyse" and "View last analysis". The dialog is overlaid on the same file upload page as seen in the previous screenshot.

### Current Scan Results

SHA256:	0bfe80a8daf892eaod40a979b190a28a34fe4fc4d1eef238d1654811b9d1a315	
File name:	denied.shtml	
Detection ratio:	5 / 41	
Analysis date:	2012-07-24 12:59:43 UTC ( 1 minute ago )	

[More details](#)

Antivirus	Result	Update
AhnLab-V3	-	20120724
AntiVir	-	20120724
Antiy-AVL	-	20120724
Avast	-	20120724
AVG	-	20120724
BitDefender	-	20120724
ByteHero	-	20120723
CAT-QuickHeal	-	20120724
ClamAV	-	20120723
Commtouch	-	20120724
Comodo	UnclassifiedMalware	20120724
DrWeb	-	20120724
Emsisoft	Trojan.IframeRef!IK	20120724

### Additional Details

**ssdeep**  
192:qC0tYEtnC0GosYYhYQDN3mMwymTFPMvAlngtkN:qC0eEgzv4P+ISM

**TrID**  
Unknown!

**First seen by VirusTotal**  
2011-09-09 20:54:51 UTC ( 10 months, 2 weeks ago )

**Last seen by VirusTotal**  
2012-07-24 12:59:43 UTC ( 2 minutes ago )

**File names (max. 25)**

- a
- p.jpg
- denied.shtml
- 04.exe
- bffb82fc0b49527a4d7adea31c588986.shtml
- file-2769709\_.shtml

On top of the manual submission interface, VirusTotal also provides an API (<https://www.virustotal.com/documentation/public-api/>) that can be used for automating the submission and result analysis process. The API is HTTP based and uses simple POST requests and JSON replies. We used a set of homegrown Python scripts to schedule an automated scan of all the samples in our data set on a weekly basis. Results were stored in a relational database for further analysis. We ran the experiment for six weeks and collected a total of 13,000 entries in our database, where each entry represents the result of a specific scan of a specific sample file by a specific product.

## Analyzing the Results

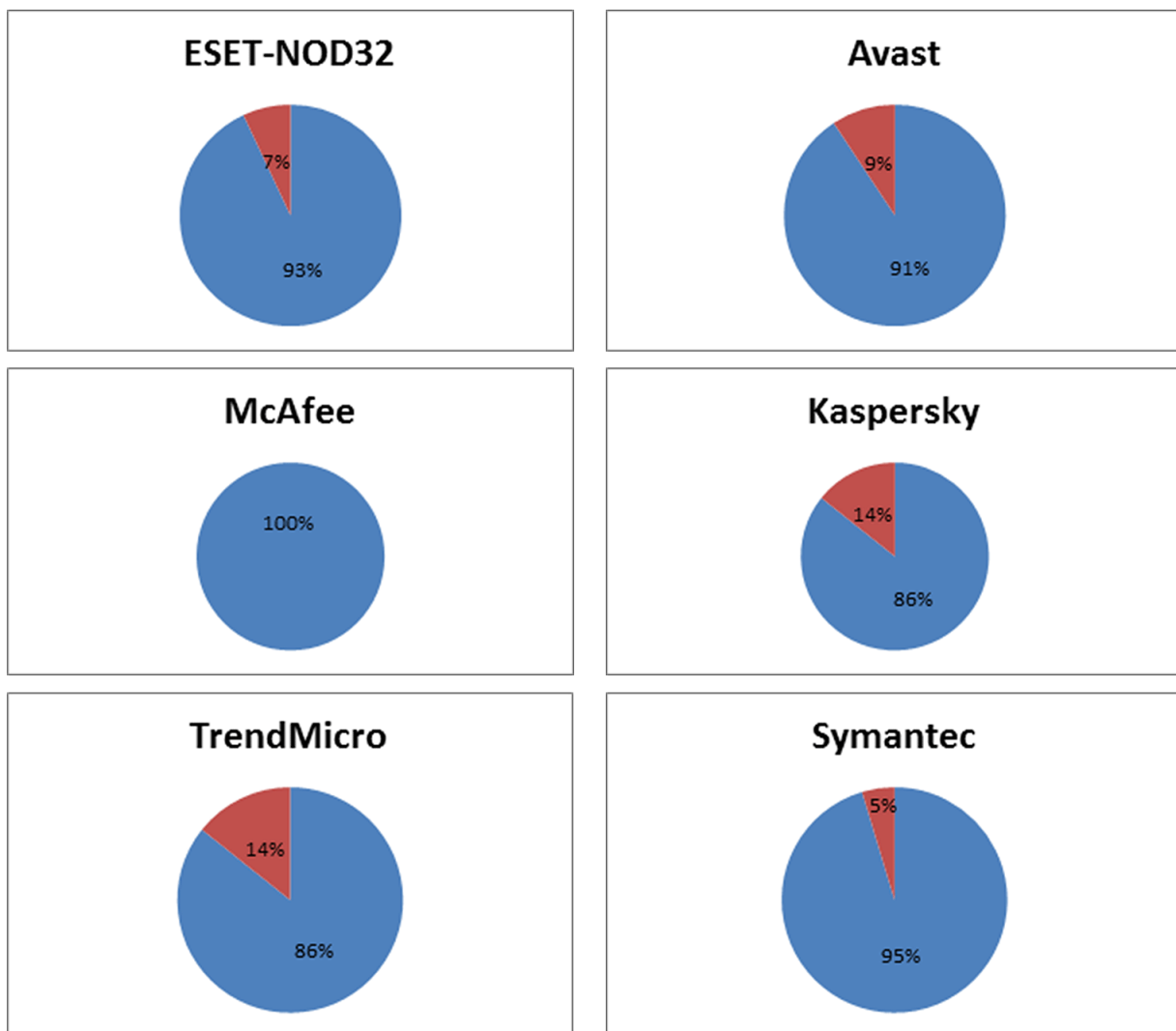
### General Statistics

In our analysis, we looked at two types of measurements: static and dynamic. The static measurements look at AV coverage regardless of the timeline. The dynamic measurements look at the evolution of AV coverage over time.

The first measurement we took is coverage by most popular AV products (see above). For this static measurement, we picked up both commercial and free AV products and looked only at those samples that, by the end of the testing period, were identified by at least 50% of evaluated products (we used this criteria to reduce noise and potential dispute claims).

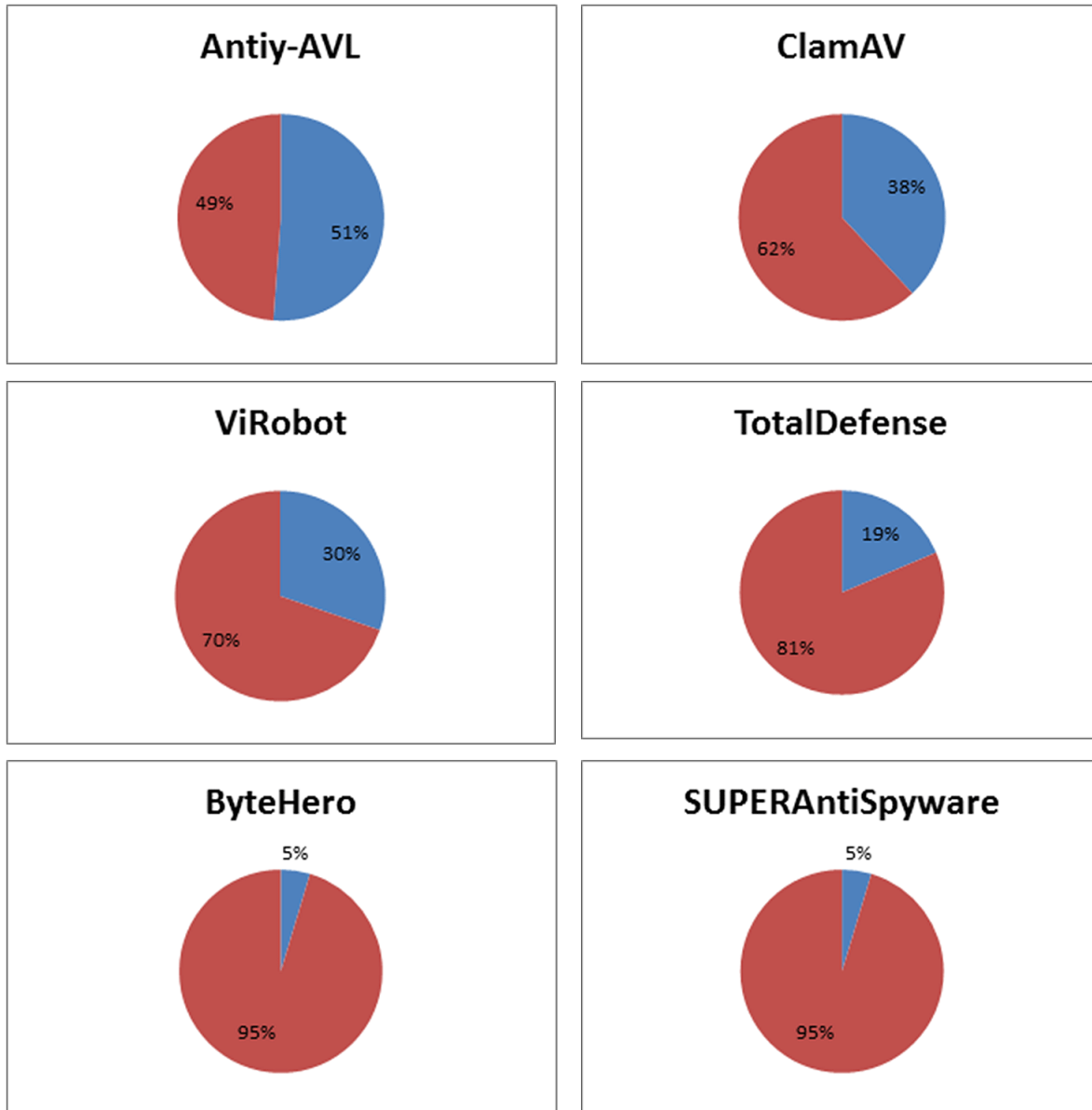
The results are displayed in Table 1 where blue area matches the portion of the sample that was detected.

**Table 1: Viruses Identified vs. Not Detected, by Antivirus Vendor**



Tables 1-2 show the rate of detection by **the 6 least effective antivirus products** in our study relative to the group of files in which more than 50% of antivirus products that were tested identified the viruses (during the final scan). Notice that some of the products in this group are commercial products for which customers actually pay license fees.

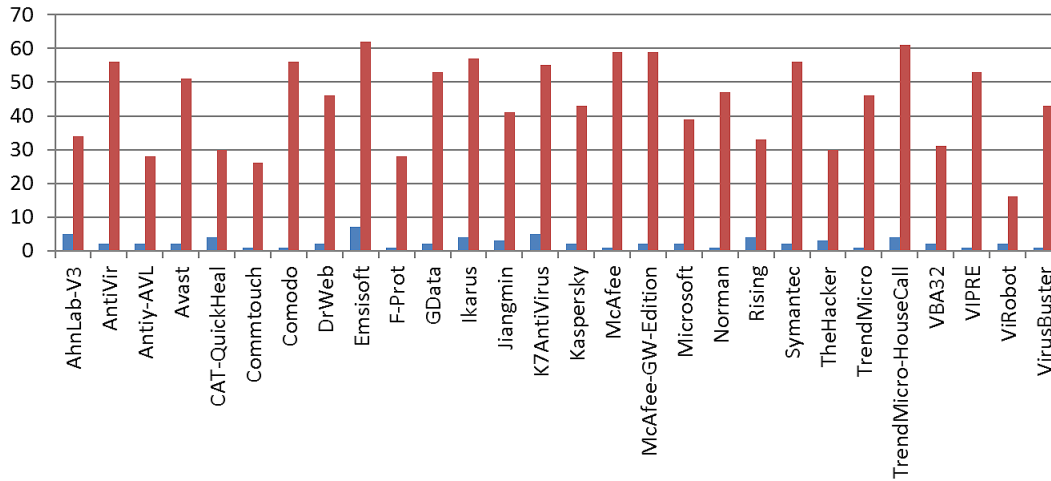
**Table 2: Least Effective Products**





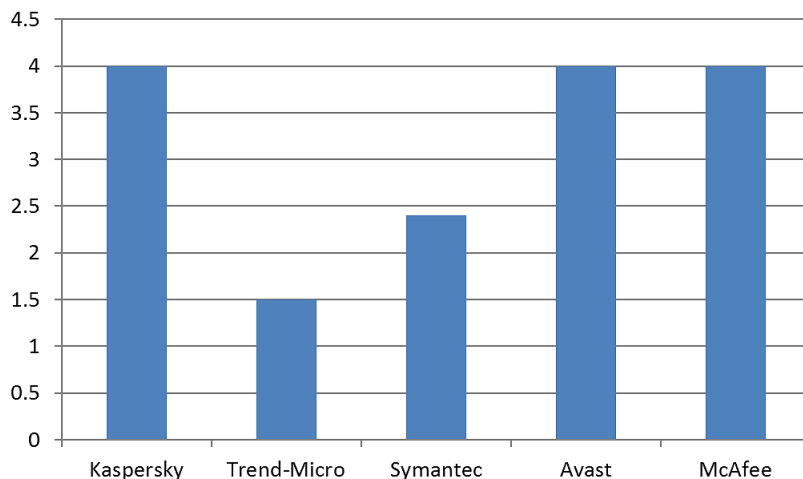
Our first dynamic measurement compares each AV product's detection capability at the beginning of the test (first run, colored in blue) with its detection rate at the end of the test (last run, colored in red). It indicates how well AV products process new inputs in general. The diagram below includes only those products for which an improvement was shown. The diagram shows that AV products, indeed, are highly dependent on their input, and most products, in fact, have a solid process of turning their input into detection signatures.

**Table 3: Virus Detection between First and Last Run, by Antivirus Vendor**



Now we get to the very interesting question of how long does it take for an AV product to incorporate detection for a previously undetected sample. The following chart shows the average time, by the vendor listed, to detect those samples that were not recognized as malware in the first run. For each vendor, we took the average for files not detected by that vendor alone. We chose to show the progress rate only for the most prominent product out there. We chose the AV with biggest market share (AVAST) and then 4 commercial products from the largest Security / AV vendors. The data in this chart gives us an idea about the size of the "window of opportunity" for an attacker to take advantage of a freshly compiled malware. Do notice that none of the malware samples we used were identified by ANY of the products as an entirely new type of malware – rather, they were all recompilations of existing malware families. As one can see, the typical window of opportunity for the listed AV products is as long as four weeks!

**Table 4: Number of Weeks Required to Identify Infected File not identified in First Run**

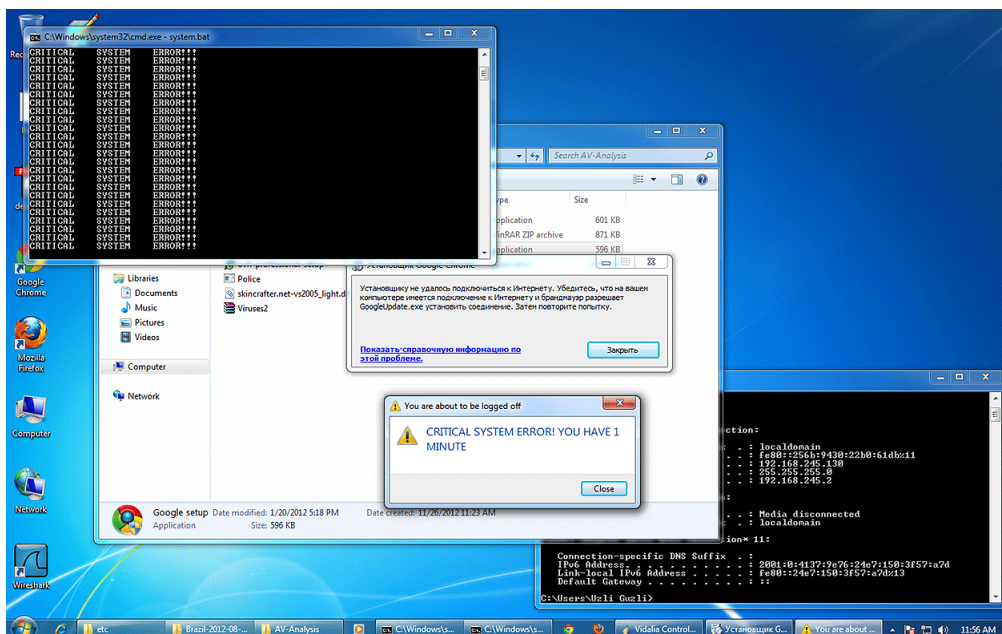


When we checked the dynamics of the least detected samples, we came up with even worse results. We checked how many weeks are required for samples to reach a rate greater than 50% detection that were detected less than 25% of the time during their initial scan. By analyzing our results database, we discovered that 12 files had a detection rate of less than 25% when they were first scanned, yet not a single one of them came close to being detected 50% of the time in following scans. Another phenomenon that we discovered after analyzing the results, which were obtained across the period of a few weeks and after scanning was finished, was that not only did detection change, but the association made by antivirus products changed. This means that we encountered a situation in which, over the period of three weeks, antivirus products classified a file as “Unclassified Malware,” and only in the fourth week did it finally classify it as a specific type of malware (Trojan Horse). We additionally encountered cases in which the antivirus completely changed the classification that it made of a specific file. For example, one week the antivirus product ByteHero identified a file as *Trojan Malware*, and another as *Virus. Win32*. Consequently, we can conclude that antivirus products occasionally are not consistent in the results they provide. In our analysis, we have tried to come up with an effective combination of AV products that would yield the best protection against our data set. We have considered, for the sake of this experiment, only those files that were detected by more than 25% of AV products. None of the individual AV products were able to provide coverage for this set of samples. To our surprise, the set of antivirus products that has the best detection rates included two freeware antivirus products, Avast and Emsisoft. Another interesting point is that, while the most well-known AV products provided the best standalone coverage, their coverage could not be effectively enhanced using another single product.

## Specific Samples

### Fake Google Chrome Installer

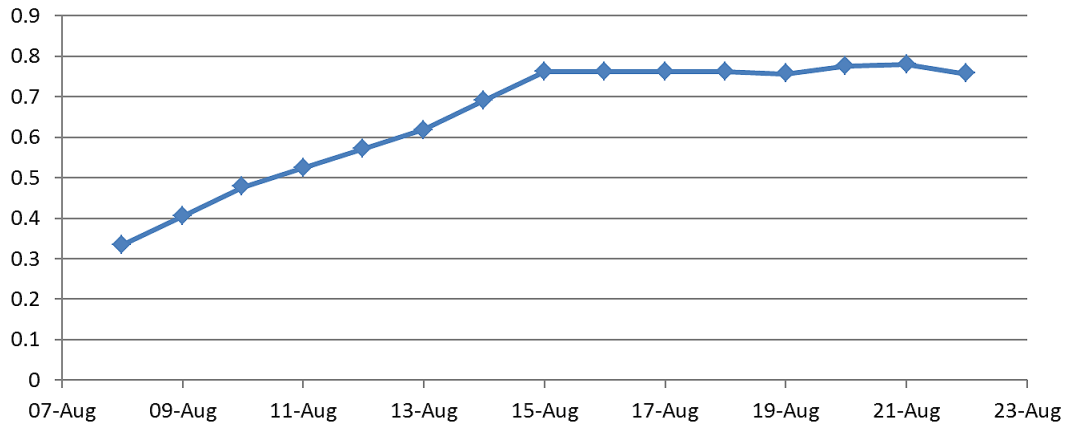
One of the samples in our data set was a fake Google Chrome installer name “Google setup.exe.” When executed, it attempts to access a command and control center and takes over important functionality, closing down many programs and, in particular, preventing the user from opening the “Task Manager” tool (which is an attempt to hide the presence of a rogue process in the system). Below, we can see a screenshot of some of the (very apparent) visual effects observed when executing this malware. The file was first reported to VirusTotal.com and analyzed on February 9, 2012. Yet, by the end of our study, only 20 out of 42 products were able to detect it. By November 17, 2012, only 23 of 42 products were able to detect it. Only a portion of those products that do detect it actually identify it correctly as being a disabler/dropper.



### Multipurpose Trojan with Fake AV

“Hot\_Girls\_Catalog\_2012\_August.zip” is one of the samples we chose to track individually, that we picked up from a large Phishing campaign. We decided to put some emphasis on it because we knew it was quickly spreading through the web and thus must have captured the attention of AV product developers. The file contains a general purpose Trojan (of the Kulouz family), capable of communicating with a larger highly redundant network of C&Cs. The Trojan receives execution modules and configuration files from its C&C and has been known to grab passwords, send out spam, attack other servers, and display Fake AV to the user. We tracked the detection rate for this sample on a daily basis for two weeks. As can be seen from the chart below, the initial detection rate of the sample is around 30% of AV products. The sample is quickly picked up by AV vendors through the first week and detection rate settles to just below 80% after that. A few other recompilations of the same malware that were distributed in the same campaign did not reach more than 40% detection during the time frame of the study, evading even some of the most popular AV products. Detection rate for those variations also eventually settled near 80%.

**Table 5: Kulouz Sample Rate of Detection Over Time**



## Conclusion

The issue of antivirus effectiveness is something close to us. There's no doubt that many of us have lost both information and wasted time trying to recover after a virus succeeded in infecting our computers. Sadly, an industry exists to produce new viruses on a massive scale, making antivirus products mostly unreliable. Attackers understand antivirus products in depth, become familiar with their weak points, identify antivirus product's strong points, and understand their methods for handling the high incidence of new virus propagation in the Internet.

The question also arises regarding how a virus manages to sneak by and cause damage when a leading antivirus product is installed on our computer. There are several conclusions:

1. Antivirus products (as demonstrated by our study and by incidents like Flame) are much better at detecting malware that spreads rapidly in massive quantities of identical samples, while variants that are of limited distribution (such as government sponsored attacks) usually leave a large window of opportunity.
2. The window of opportunity mentioned in the preceding bullet point creates a massive blind spot for security teams. For example, when attackers breached the state of South Carolina, the attack went unnoticed because the security team was not able to monitor and control data access across DoRs internal network and servers, making them the cyber equivalent of deaf and blind to the attack. They likely had antivirus technology intended to block the initial infection. When their first line of defense was breached, due to antivirus' limitations, they were left unaware and defenseless against the attack.
3. A new security model is required to cover this blind spot. Investing in the right "ears and eyes" to monitor the access of servers, databases, and files, would make the detection of malware attacks an easier task, as many attacks are very "noisy." In many cases, attackers seek access to privileged data on an arbitrary time from an arbitrary process with read permissions, while usually the data gets accessed only by the internal backup process, with the backup account privileges, on the regular backup times with write permissions. In the case of South Carolina, for example, the attacker moved and processed the data many times before sending it out of the network, giving a lot of missed chances to set off an alarm.

## Limitations, Objections and Methodology

VirusTotal did not participate in our study. VirusTotal indicates that its services were not designed as a tool to perform antivirus comparative analyses, and that there are many implicit errors in methodology when using VirusTotal to perform antivirus comparative analyses. Implicit errors include the following:

1. VirusTotal AV engines are commandline versions, so depending on the product, they will not behave quite like the desktop versions.
2. VirusTotal desktop-oriented solutions coexist with perimeter-oriented solutions; heuristics in this latter group may be more aggressive and paranoid, since impact of false positives is less visible in the perimeter.

Several objections can be and have been raised regarding this study:

**Objection #1:** VirusTotal was used for comparative purposes.

The essence of the report is not a comparison of antivirus products. Rather, the purpose is to measure the efficacy of a single antivirus solution as well as combined antivirus solutions given a random set of malware samples.

**Objection #2:** Our random sampling process is flawed.

Instead of testing a huge pile of samples taken from databases or standard antivirus traps, we looked for samples in a limited manner which is not biased in any way towards a specific type of malware. Our selection of malware was not biased but was randomly taken from the Web reflecting a potential method for constructing an attack. We believe our approach is an effective approach since this reflects how malware writers create malware variants constantly. Our methodology closely mimics what most enterprises or consumers encounter especially in an APT scenario.

## References

<https://www.virustotal.com/documentation/public-api/>

<http://www.securitylab.ru/>

<http://wiki.python.org/moin/BeginnersGuide>

<http://docs.python.org/library/json.html>

<http://www.pyp.co.il>

## Hacker Intelligence Initiative Overview

The Imperva Hacker Intelligence Initiative goes inside the cyber-underground and provides analysis of the trending hacking techniques and interesting attack campaigns from the past month. A part of Imperva's Application Defense Center research arm, the Hacker Intelligence Initiative (HII), is focused on tracking the latest trends in attacks, Web application security and cyber-crime business models with the goal of improving security controls and risk management processes.