Measuring the in-the-wild effectiveness of Antivirus against Zeus

Trusteer

September 14, 2009

Introduction

There are many reports on how anti-virus products fare against malware, yet most of these reports focus on in-the-lab testing of specific malware strands against a specific antivirus configuration. Very little is said about the situation in the field – where malware distribution statistics (and to some extent, antivirus distribution statistics) are unclear.

Trusteer is uniquely positioned in a way that enables it to get a comprehensive view of consumer world PCs – Trusteer Rapport is installed on millions of consumer PCs and reports statistics of malware infection and security software installed.

We chose to focus on Zeus (also known as Zbot, WSNPOEM, NTOS and PRG) as it tops the list of financial Trojans. In other words, Zeus is probably the most painful financial malware out there, both in terms of infection size, and in terms of effectiveness.

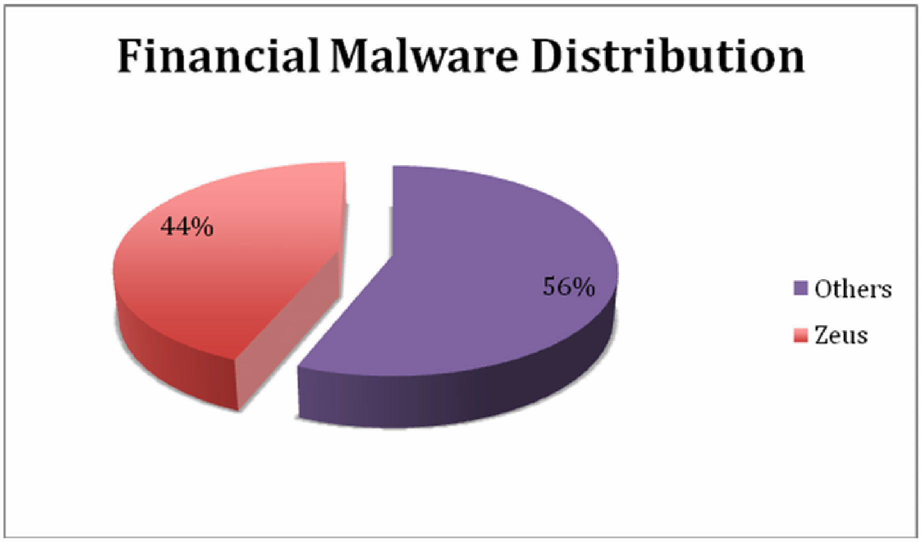
About Zeus

Zeus is a financial malware. It infects consumer PCs, waits for them to log onto a list of targeted banks and financial institutions, and then steals their credentials and sends them to a remote server in real time. Additionally, it may inject HTML into the pages rendered by the browser, so that its own content is displayed together (or instead of) the genuine pages from the bank's web server. Thus, it is able to ask the user to divulge more personal information, such as payment card number and PIN, one time passwords and TANs, etc.

Zeus uses some rootkit techniques to evade detection and removal.

Zeus is the #1 botnet, with 3.6 million PCs infected in the US alone (i.e. approximately 1% of the PCs in the US), according to a recent report[1]. This is backed by Trusteer'sfield figures as well, as can be seen in the following pie chart of relative financial malware distribution:

[1] http://www.networkworld.com/news/2009/072209-botnets.html



Methodology

Our research is based on statistics gathered from Rapport agents running on users' PCs. Rapport detects Zeus through a unique fingerprint left by Zeus when it penetrates the browser process. This fingerprint is an inherent part of Zeus's modus operandi.

Rapport detects the existence of antivirus products and whether they're up-to-date via the Windows Security Center. Note that some antivirus solutions do not report to the Windows Security Center. In this scenario we categorize the machine as not having an antivirus. This means that the real number of users who are infected with Zeus and run an up-to-date antivirus is actually bigger than the number we detected, indicating that the problem is even worse than our findings.

Raw statistics

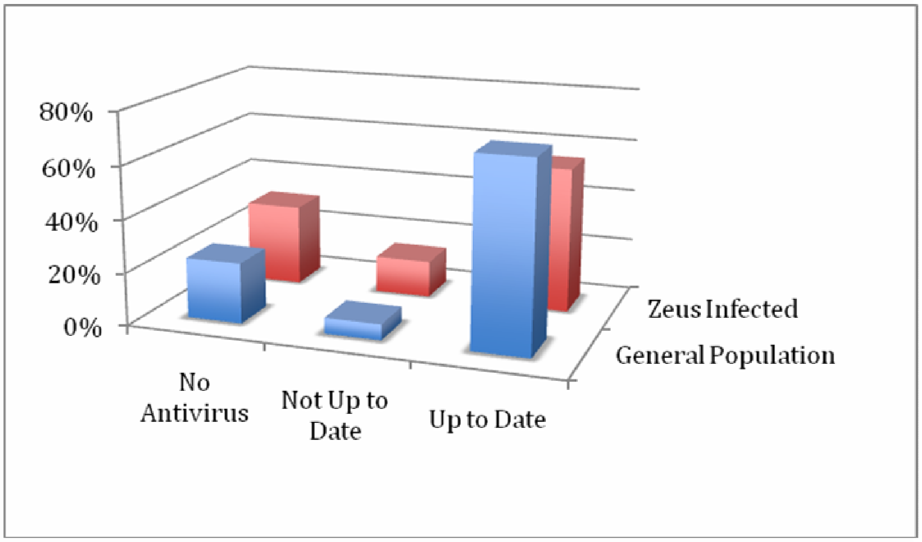
The following data has been collected from consumer PCs during one day in September 2009:

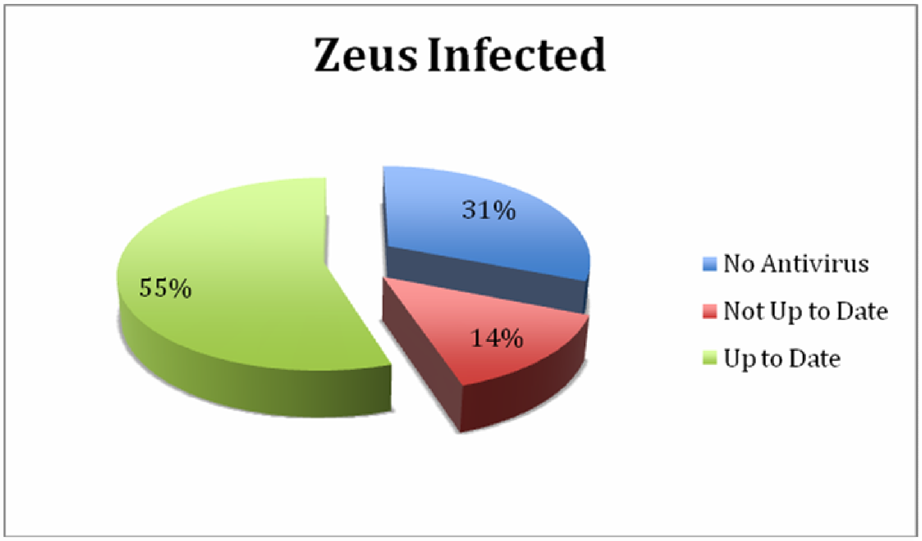
	General Population	Zeus-infected
No Antivirus found	23%	31%
Antivirus found but not up-to-date	6%	14%
Antivirus is up-to-date	71%	55%

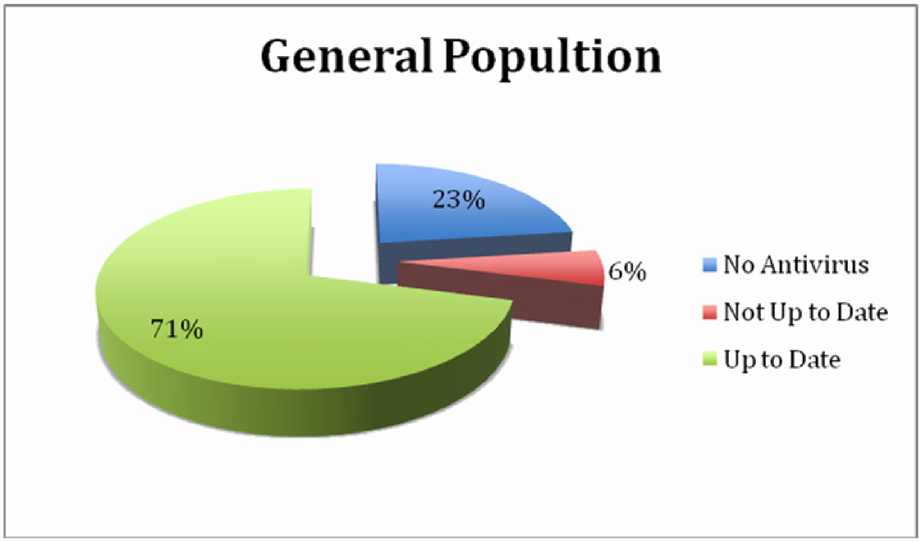
The Zeus-infected population we sampled consisted of 10,000 machines.

A quick glimpse at this table already reveals a disturbing phenomenon – the majority of Zeus infections occur on machines which have an installed an up-to-date anti-virus product.

The distribution of antivirus products we observed on infected and clean machines is pretty constant and therefore we cannot attribute infections to a specific set of antivirus products that perform less effectively than the others.







Quantitative Analysis

The data above enables us to calculate the efficiency of anti-virus products at large, as well of that of specific products.
To this end, we can employ the Bayesian theorem:

AVUTD = Antivirus is up-to-date
NoAV = No antivirus found

$p(Zeus|AVUTD)=p(AVUTD|Zeus)*p(Zeus)/p(AVUTD)$
$p(Zeus|NoAV)=p(NoAV|Zeus)*p(Zeus)/p(NoAV)$

Dividing both sides, we obtain the following ratio:

$p(Zeus|AVUTD)/p(Zeus/NoAV)=(p(AVUTD|Zeus)*p(NoAV))/(p(AVUTD)*p(NoAV|Zeus))$

We can now substitute values:

$p(AVUTD|Zeus)=0.55$
$p(NoAV|Zeus)=0.31$
$p(AVUTD)=0.71$
$p(NoAV)=0.23$

This yields:

p(Zeus|AVUTD)/p(Zeus|NoAV)=0.77

In other words, installing an anti-virus product and maintaining it up to date reduces the probability to get infected by Zeus by 23%, compared to running without an anti-virus altogether. The effectiveness of an up to date anti virus against Zeus is thus not 100%, not 90%, not even 50% - it's just 23%.

Conclusion

We measured the efficiency of antivirus products in the wild, against Zeus. In a sense, it's more accurate than in-the-lab experiments, since it measures the real phenomenon – the actual infections in the wild, vs. real antivirus deployment in the wild. The result we measured, efficiency level of 23%, is disturbing, and reveals that the vast majority of Zeus infections go unnoticed by antivirus products.