Viruses, Spam and Spyware - AKA Malware

May 2010

Two new topics:
Botnets and Rootkits

Paul Lewis

Route-plan

- Why do we bother to protect our computer?
- The weakest link in the protection shield
- Something more to worry about
  - Rootkits
  - Botnets
- The latest test results from PC World
  - Internet Security Suites
  - Microsoft Security Essentials
- What to do

A Reminder - Why should I bother?

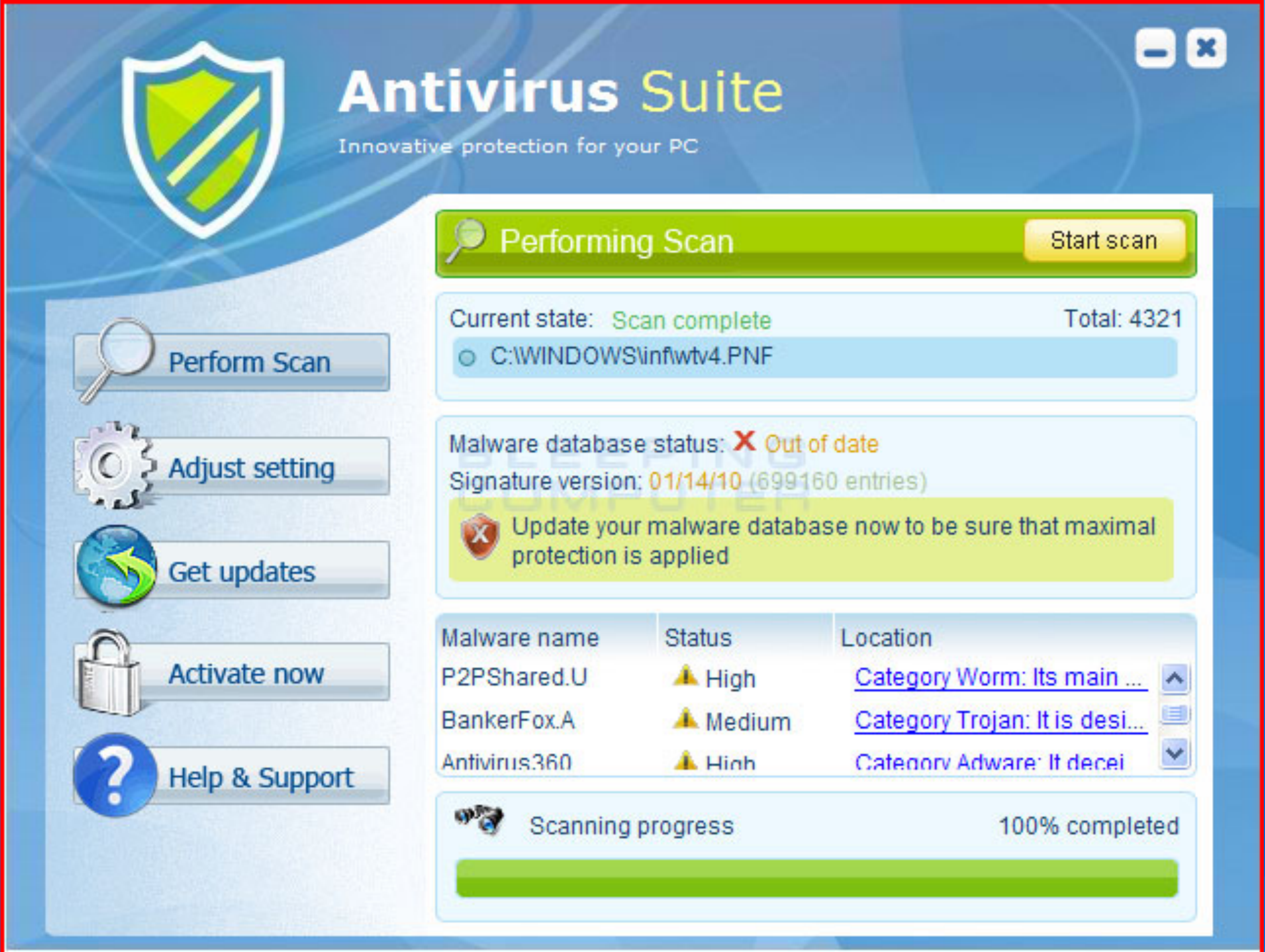
- Identity theft
- Bank fraud
- Online scams
- Your computer is used for fraudulent transactions - without your permission or knowledge
- Computer repair costs

Things Don't Always Improve

The year 2009 was a bad one for PC security:

Online attackers created more malware last year than in the previous 20 years combined.

Sample Scare-ware - fake antivirus



Current state: Scan complete Total: 4321

○ C:\WINDOWS\inf\wtv4.PNF

Malware database status: ✗ Out of date

Signature version: 01/14/10 (699160 entries)

Update your malware database now to be sure that maximal protection is applied

Malware name	Status	Location
P2PShared.U	⚠ High	Category Worm: Its main ...
BankerFox.A	⚠ Medium	Category Trojan: It is desi...
Antivirus360	⚠ High	Category Adware: It decei

Scanning progress 100% completed

Antivirus Suite screen shot
For more screen shots of this infection click on the image above.
There are a total of 8 images you can view.

Scareware: Most Costly Security Scam of 2010

Fake antivirus programs that encourage Web users to part with their hard-earned cash and download hoax security software is likely to be the most costly scam of 2010, says McAfee.

According to the security firm, cybercriminals make upwards of $300 million from conning web users worldwide into downloading scareware.

The security firm also said it had seen a 660 percent rise in scareware over the past two years, and a 400 percent increase in reported incidents in the last 12 months.

The Weakest Link - You

Many sources advise that the weakest link in your protection is YOU!

- What you **DO** sitting at your computer -
  - Many incidents occur because the user is tricked into clicking where they shouldn't - called "social engineering"
- What you **Fail to do** to keep your computer protected
  - Keep all programs up to date - especially
    - Windows XP - Vista, Windows 7
    - Internet Explorer / Firefox / Chrome /
  - Use more than one protection program
    - ONE antivirus and one or two other antimalware scanners
  - Have your computer(s) behind router/ firewall

The burglar alarm analogy

Even if you have:

- Locks on your doors and windows
- Detection-switches on doors and windows
- Motion detectors
- Outside siren
- Auto-response team

If "someone" in the house lets a stranger in at the back door - who watches and memorises how you turn off the alarm system - (Or you fail to turn on the alarm system when you leave the house)

ALL BETS ARE OFF!

Rootkits

What are they?

What do they do?

Why do they do it?

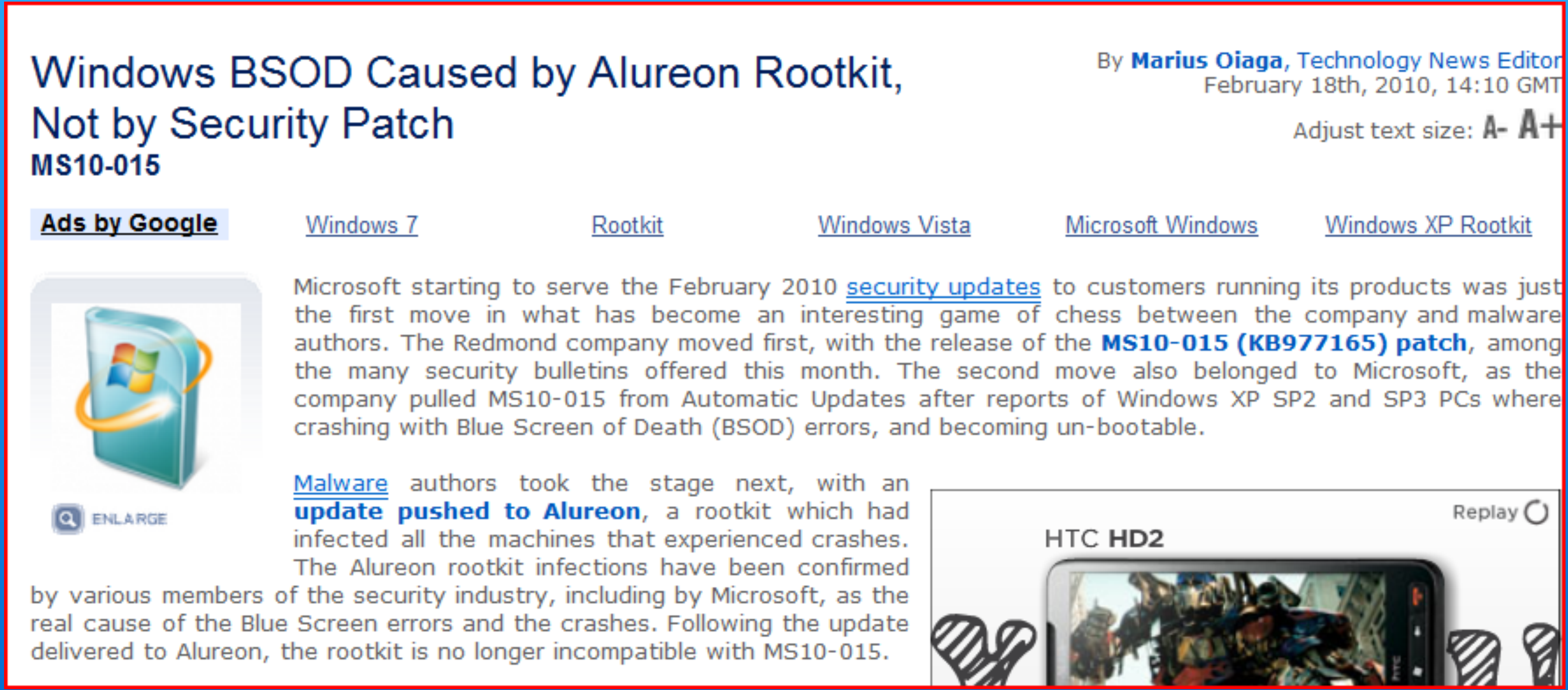
Current Security Suite - Feature-set

Almost all the security suites we tested this year also include *some form* of **antirootkit** technology.

Rootkits--a kind of stealth malware used to hide infections--were once the concern only of big businesses, but they have gradually become more commonplace

All the suites we reviewed had anti virus, antispyware, and antispam components, plus a firewall. (Some have "in the cloud" features)

Rootkit Battles MS Update - BSD



Windows BSOD Caused by Alureon Rootkit, Not by Security Patch

MS10-015

By **Marius Oiaga**, Technology News Editor
February 18th, 2010, 14:10 GMT

Adjust text size: A- A+

Ads by Google Windows 7 Rootkit Windows Vista Microsoft Windows Windows XP Rootkit

Microsoft starting to serve the February 2010 security updates to customers running its products was just the first move in what has become an interesting game of chess between the company and malware authors. The Redmond company moved first, with the release of the **MS10-015 (KB977165) patch**, among the many security bulletins offered this month. The second move also belonged to Microsoft, as the company pulled MS10-015 from Automatic Updates after reports of Windows XP SP2 and SP3 PCs where crashing with Blue Screen of Death (BSOD) errors, and becoming un-bootable.

Malware authors took the stage next, with an **update pushed to Alureon**, a rootkit which had infected all the machines that experienced crashes. The Alureon rootkit infections have been confirmed by various members of the security industry, including by Microsoft, as the real cause of the Blue Screen errors and the crashes. Following the update delivered to Alureon, the rootkit is no longer incompatible with MS10-015.

Replay
HTC **HD2**

http://news.softpedia.com/news/Windows-BSOD-Cause-by-Alureon-Rootkit-Not-by-Security-Patch-135407.shtml

What is a Rootkit?

A rootkit is a set of software tools frequently used by a third party (usually an intruder) after gaining access to a computer system.

The tools are are intended to conceal running processes, files or system data, which allows the intruder **maintain access to a system without the user's knowledge.**

After the "Bloodless Coup"

A common abuse is to use a compromised computer as a staging ground for further abuse. This is often done to make the abuse **appear to originate from the compromised system** or network instead of the attacker.

Tools for this can include denial-of-service attack tools, tools to relay chat sessions, and e-mail spam attacks.

http://www.infopackets.com/news/technology/word_of_the_day/2009/20090527_rootkit.htm

Removing Root-kits

Many feel that removing a rootkit is forbiddingly impractical.

Even if the nature and composition of a rootkit is known, the time and effort of a system administrator with the necessary skills or experience would be better spent re-installing the operating system from scratch.

Bots and Botnets

What are they?

What do they do?

Why are they so bad for the the internet?

Bots and Botnets

Bot - short for Robot (also known as a Zombie)
In computer jargon, a computer that has been "taken over" and now runs several programs automatically and is under remote-control by a "bot-master"

The owner of the computer is usually not aware that the computer has been "hijacked"

Botnet
A cluster or network - usually of tens or hundreds of thousands of bots. All members of the net are controlled remotely by the botmaster.

Big-Big Botnets

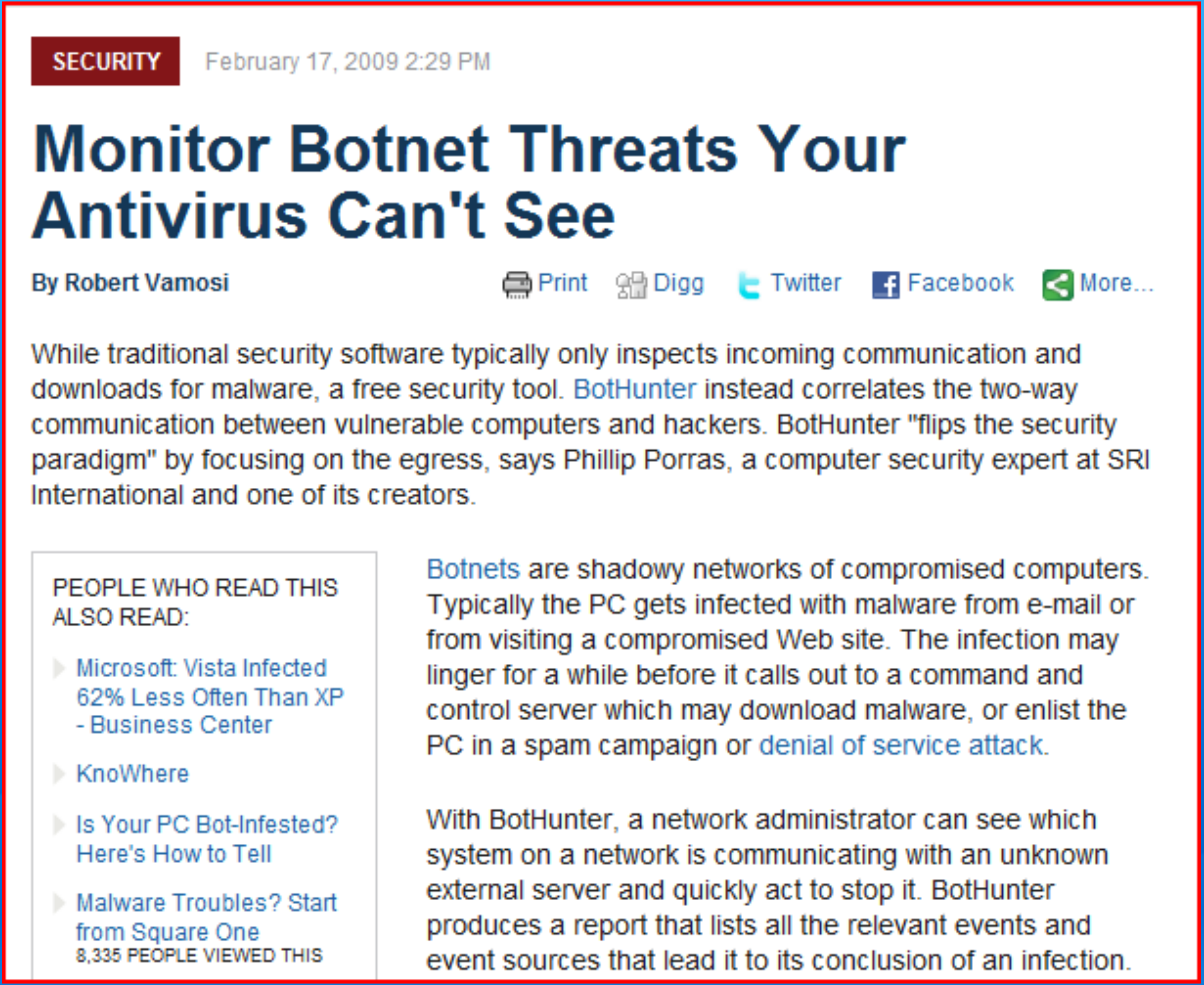
Several botnets have been found and removed from the Internet.

The Dutch police found a 1.5 million node botnet[2] and the Norwegian ISP Telenor disbanded a 10,000-node botnet.[3]

Large coordinated international efforts to shut down botnets have also been initiated.[4]

It has been estimated that up to **one quarter of all personal computers** connected to the internet may be part of a botnet.[5]

BotHunter 2



February 17, 2009 2:29 PM

Monitor Botnet Threats Your Antivirus Can't See

By Robert Vamosi

While traditional security software typically only inspects incoming communication and downloads for malware, a free security tool. BotHunter instead correlates the two-way communication between vulnerable computers and hackers. BotHunter "flips the security paradigm" by focusing on the egress, says Phillip Porras, a computer security expert at SRI International and one of its creators.

PEOPLE WHO READ THIS ALSO READ:

- Microsoft: Vista Infected 62% Less Often Than XP - Business Center
- KnoWhere
- Is Your PC Bot-Infested? Here's How to Tell
- Malware Troubles? Start from Square One

8,335 PEOPLE VIEWED THIS

Botnets are shadowy networks of compromised computers. Typically the PC gets infected with malware from e-mail or from visiting a compromised Web site. The infection may linger for a while before it calls out to a command and control server which may download malware, or enlist the PC in a spam campaign or denial of service attack.

With BotHunter, a network administrator can see which system on a network is communicating with an unknown external server and quickly act to stop it. BotHunter produces a report that lists all the relevant events and event sources that lead it to its conclusion of an infection.

Botnet Command and Control

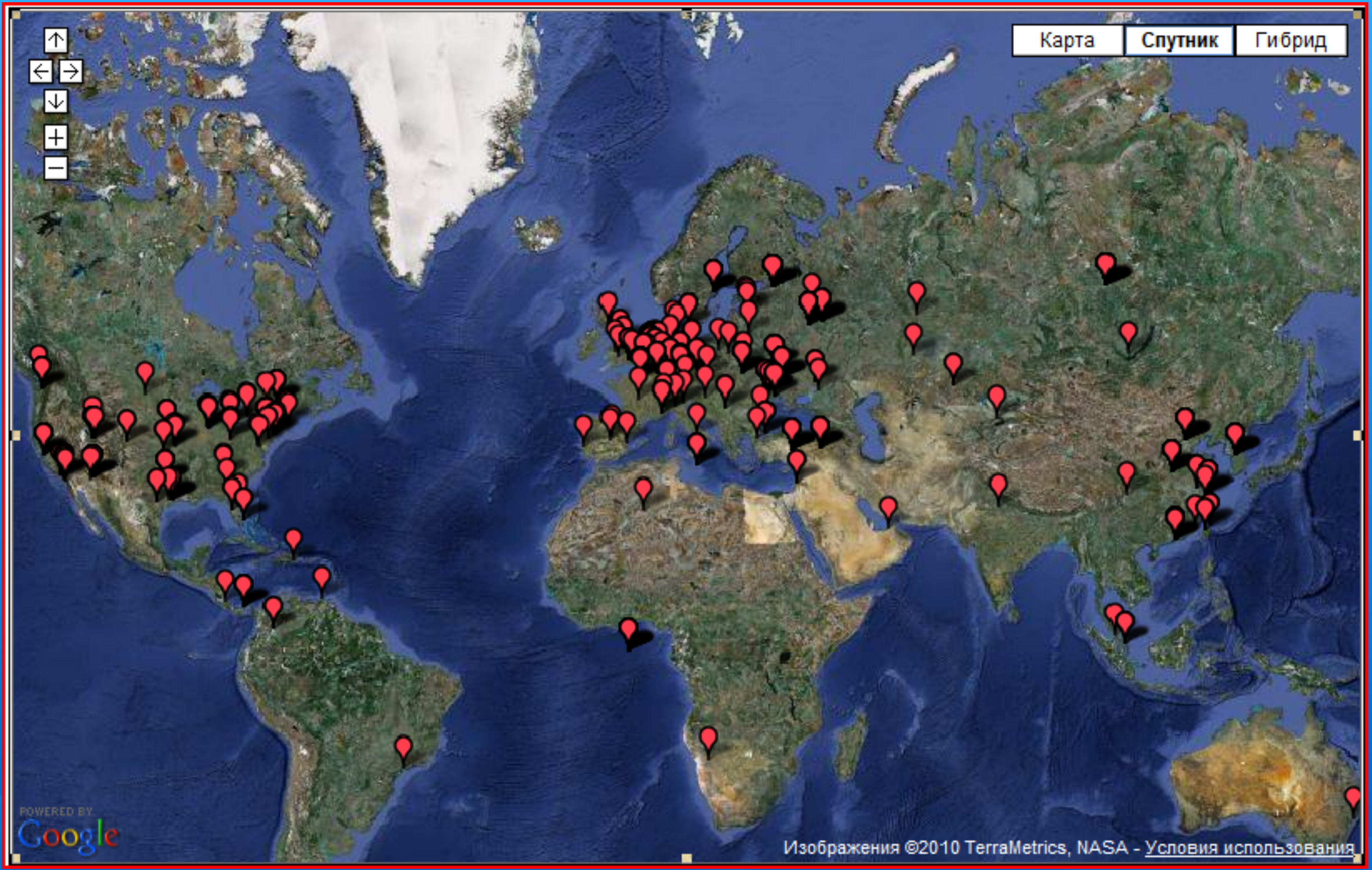

Карта
Спутник
Гибрид
POWERED BY Google
Изображения ©2010 TerraMetrics, NASA - Условия использования

Figure 1. The locations of ZBot/Zeus botnet command centers, from ZeuS Tracker data

http://www.securelist.com/en/analysis/204792115/Crimeware_A_new_round_of_confrontation_begins

Botnets - a Growth Industry

In July 2009, the ShadowServer Foundation, a group specializing in sharing information about botnets, reported that the number of identified botnets grew from 1500 to 3500 in the last two years. Each of those 3500 networks could contain several thousands of compromised PCs--and any given PC could be infected by multiple bots.

http://www.pcworld.com/article/170546/is_your_pc_botinfested_heres_how_to_tell.html?loomia_ow=t0:s0:a38:g26:r1:c0.032396:b22071294:z0

Protection

Be aware:

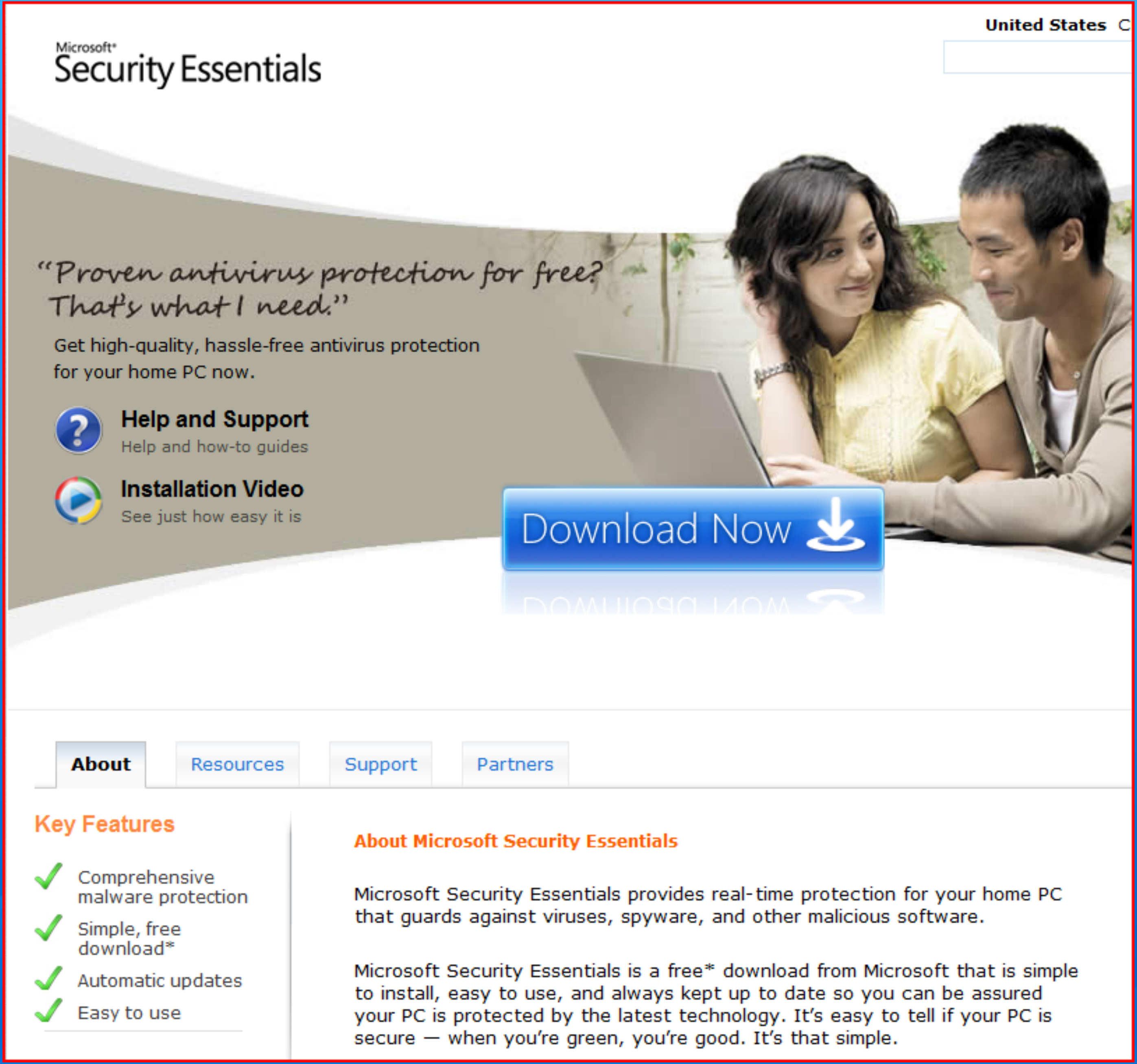
- That what you do or what you don't do contributes to your protection
- PC World reviews top three protection suites
- What else can I do?

Top Three Suites - PC World March 2010

"We tested 13 suites in all.
Norton Internet Security 2010 took the top ranking, owing to its strong overall malware detection.
Kaspersky Internet Security 2010 was a close second.
AVG Internet Security 9.0 placed third for its malware detection and speedy system performance."

http://www.pcworld.com/article/191904/maximum_security_2010_internet_security_suites.html

Microsoft Security Essentials 1



“Proven antivirus protection for free? That’s what I need.”

Get high-quality, hassle-free antivirus protection for your home PC now.

Key Features

- ✓ Comprehensive malware protection
- ✓ Simple, free download*
- ✓ Automatic updates
- ✓ Easy to use

About Microsoft Security Essentials

Microsoft Security Essentials provides real-time protection for your home PC that guards against viruses, spyware, and other malicious software.

Microsoft Security Essentials is a free* download from Microsoft that is simple to install, easy to use, and always kept up to date so you can be assured your PC is protected by the latest technology. It’s easy to tell if your PC is secure — when you’re green, you’re good. It’s that simple.

http://www.microsoft.com/security_essentials/default.aspx

Microsoft Security Essentials - Test Results June 2009

Microsoft Security Essentials: The First Test Results Are In
Nick Mediati, PC World
Jun 25, 2009 12:50 am

AV-Test coordinator Andreas Marx notes that "several other [antivirus] scanners are still not able to detect and kill all of these critters yet." In addition, Microsoft Security Essentials put up a perfect score with zero false positives—it didn't flag a single clean file as being malicious.

AV-Test also took an initial look at Microsoft Security Essentials' rootkit detection, testing it against a few rootkit samples, and found "nothing to complain about."

Microsoft Security Updates

Get the April Security Updates

http://go.microsoft.com/fwlink/?LinkId=148275

On April 13, 2010, Microsoft released **11 new** security updates for Microsoft Office, Microsoft Windows, and Microsoft Exchange Server.

http://www.microsoft.com/security/default.aspx

Free removal tools

- Microsoft Malicious Software Removal Tool
- Malwarebytes (free version)
- SuperAntiSpyware (free version)
  - Comes with some handy utilities

Recommend that you download, install, update and run at lease ONE of these soon

Thumb Rule 1

The rule of thumb:
One AntiVirus with real-time protection,

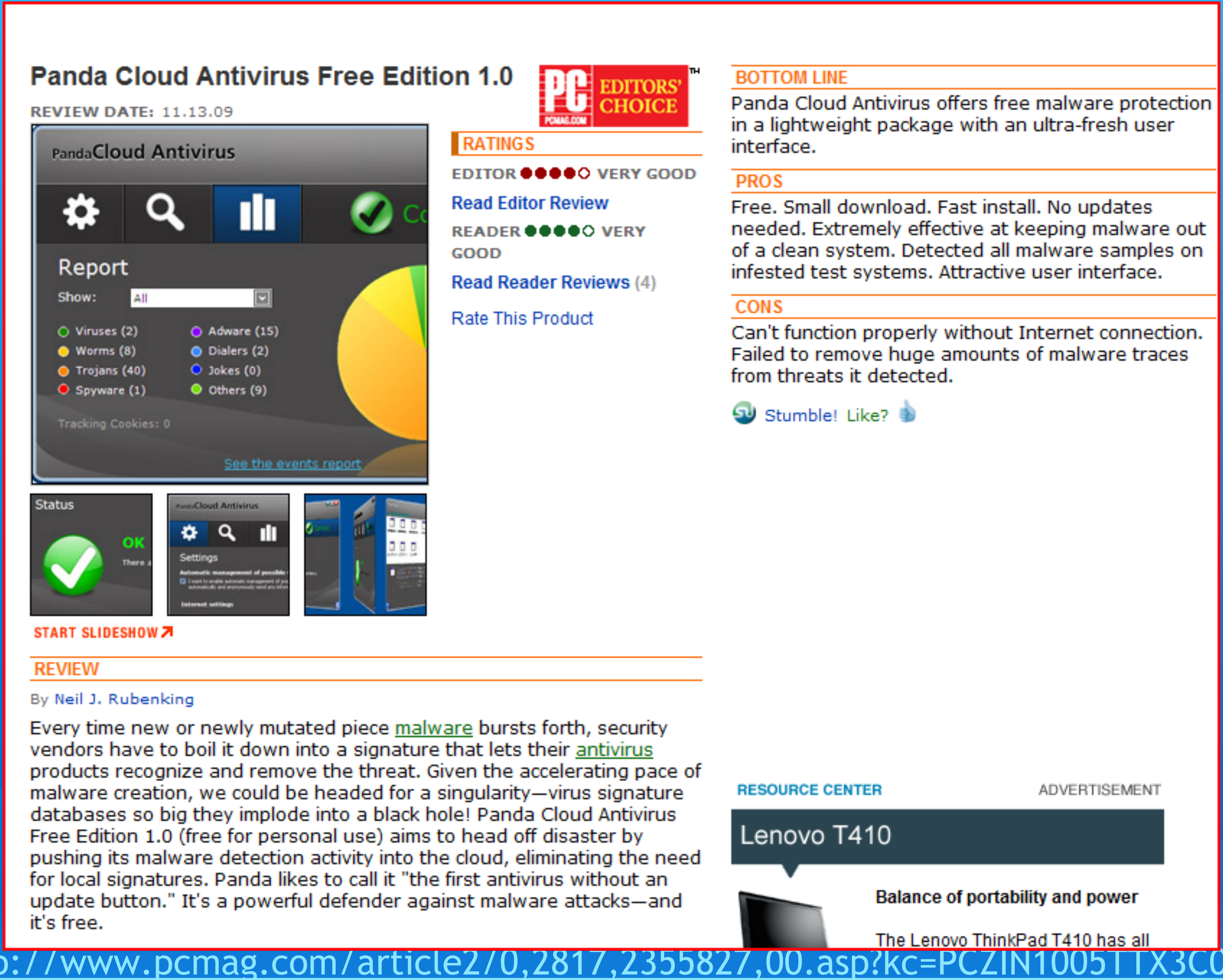
One Firewall (other than Windows firewall) and

One Antispyware with real-time protection.

Any additional anti-malware shouldn't be running. You might have two or three antispyware but they should not be running at the same time and should be set not to start with Windows.

SO...The simplest solution is to use one reputable security suite.

Panda Cloud Antivirus - free



Panda Cloud Antivirus Free Edition 1.0

REVIEW DATE: 11.13.09

START SLIDESHOW ↗

RATINGS

EDITOR ●●●●○ VERY GOOD

Read Editor Review

READER ●●●●○ VERY GOOD

Read Reader Reviews (4)

Rate This Product

BOTTOM LINE

Panda Cloud Antivirus offers free malware protection in a lightweight package with an ultra-fresh user interface.

PROS

Free. Small download. Fast install. No updates needed. Extremely effective at keeping malware out of a clean system. Detected all malware samples on infested test systems. Attractive user interface.

CONS

Can't function properly without Internet connection. Failed to remove huge amounts of malware traces from threats it detected.

Stumble! Like?

REVIEW

By Neil J. Rubenking

Every time new or newly mutated piece malware bursts forth, security vendors have to boil it down into a signature that lets their antivirus products recognize and remove the threat. Given the accelerating pace of malware creation, we could be headed for a singularity—virus signature databases so big they implode into a black hole! Panda Cloud Antivirus Free Edition 1.0 (free for personal use) aims to head off disaster by pushing its malware detection activity into the cloud, eliminating the need for local signatures. Panda likes to call it "the first antivirus without an update button." It's a powerful defender against malware attacks—and it's free.

RESOURCE CENTER ADVERTISEMENT

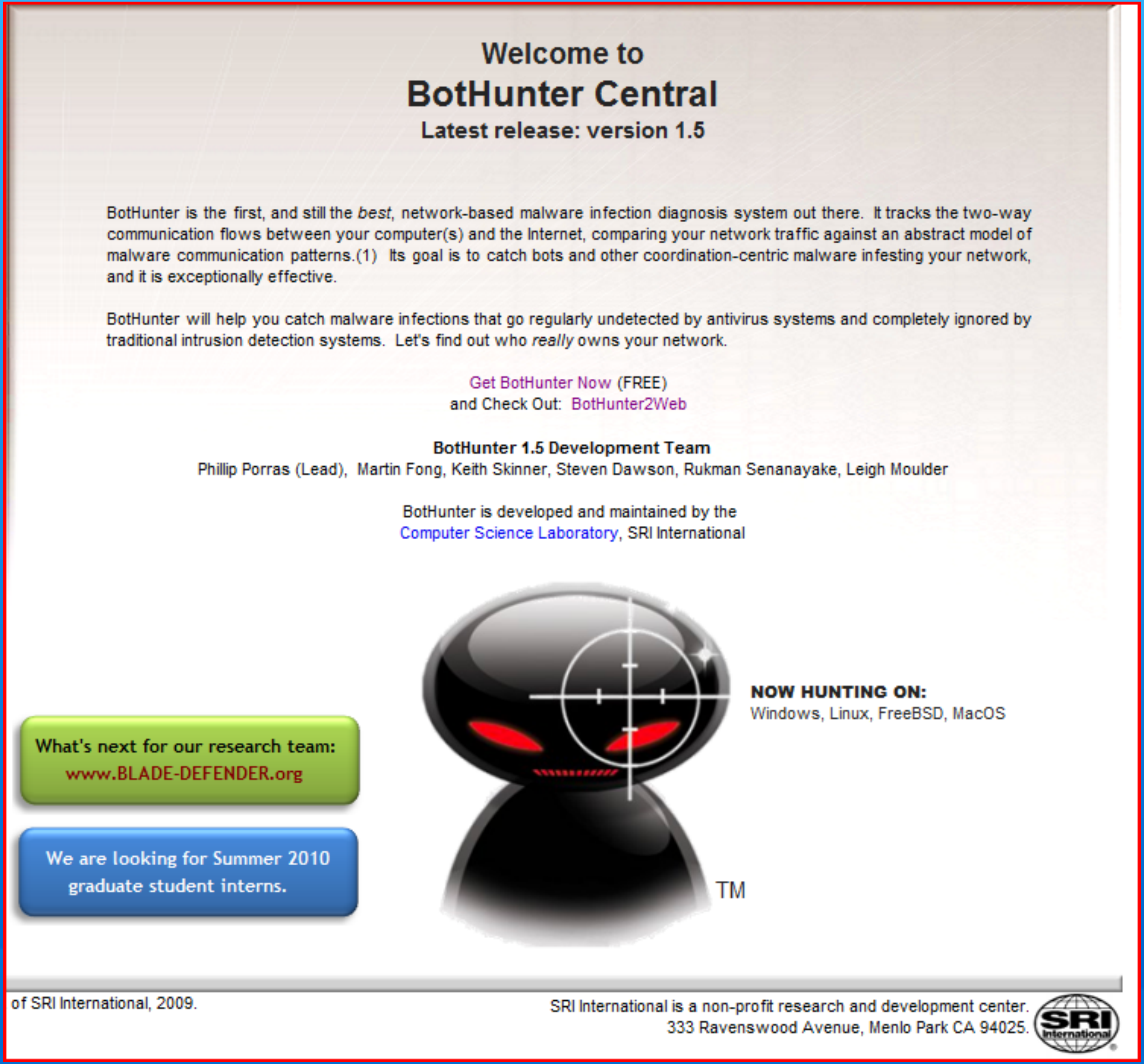
Lenovo T410

Balance of portability and power

The Lenovo ThinkPad T410 has all

http://www.pcmag.com/article2/0,2817,2355827,00.asp?kc=PCZIN1005TTX3C0001193

Bot-Hunter



Welcome to

BotHunter Central

Latest release: version 1.5

BotHunter is the first, and still the *best*, network-based malware infection diagnosis system out there. It tracks the two-way communication flows between your computer(s) and the Internet, comparing your network traffic against an abstract model of malware communication patterns.(1) Its goal is to catch bots and other coordination-centric malware infesting your network, and it is exceptionally effective.

BotHunter will help you catch malware infections that go regularly undetected by antivirus systems and completely ignored by traditional intrusion detection systems. Let's find out who *really* owns your network.

Get BotHunter Now (FREE)
and Check Out: BotHunter2Web

BotHunter 1.5 Development Team
Phillip Porras (Lead), Martin Fong, Keith Skinner, Steven Dawson, Rukman Senanayake, Leigh Moulder

BotHunter is developed and maintained by the
Computer Science Laboratory, SRI International

What's next for our research team:
www.BLADE-DEFENDER.org

We are looking for Summer 2010 graduate student interns.

NOW HUNTING ON:
Windows, Linux, FreeBSD, MacOS

of SRI International, 2009.

SRI International is a non-profit research and development center.
333 Ravenswood Avenue, Menlo Park CA 94025.

http://www.bothunter.net/
Installing on Windows

Government - Computer Safety Tips

http://www.boston.com/bostonglobe/ideas/articles/2010/04/11/please_do_not_change_your_password/?page=2 For instance, the federal government's website for computer safety tips, www.us-cert.gov, includes more than 50 categories under the heading of "Cyber Security Tips." Each category leads to complex sets of instructions.

Related web sites -1

http://blogs.techrepublic.com.com/itdojo/?p=1662&tag=nl.e101

BBC Link to Windows patch not being applied to Rootkit-infected machines
http://news.bbc.co.uk/2/hi/8624560.stm

Microsoft Malicious Software Removal Tool"
http://www.microsoft.com/security/malwareremove/default.aspx
http://www.virusbtn.com/vb100/archive/results?display=summary

http://www.theregister.co.uk/2009/08/06/vista_anti_virus_tests/

Related web sites - 2

Example of a tortuous removal process:
http://www.bleepingcomputer.com/forums/topic243996.html

Recipe for removing malware:
http://www.geekstogo.com/forum/Malware-Spyware-Cleaning-Guide-t2852.html

http://blogs.pcmag.com/securitywatch/2009/12/av-testorg_releases_real-world.php

http://www.av-comparatives.org/

http://www.virusbtn.com/vb100/rap-index.xml

http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1506416,00.html?track=NL-422&ad=758259USCA&asrc=EM_NLT_11215529&uid=8707115

https://www.opendns.com/dashboard/myaccount/