Essential Security against Evolving Threats

The Leader in Proactive Threat Protection

Disclaimer

randy

- The Views and opinions presented are strictly those of the author and do not reflect the views and opinions of his employer
- They do represent the views and opinions of a former Microsoft employee
- Some views and opinions may coincide with those of current and former Microsoft employees
- Some views may not coincide with anyone else's

MICROSOFT ANTIVIRUS

- Extension

Who Am I?

- Worked at MS from April 1993 to June 2005
  - 7 Years ensuring MS didn't release infected software
  - Participated in the creation of the Virus Information Alliance
  - Participated in the MS/ICSA MVI forum
  - 9 month with GIAIS working closely with the MSRC
- Joined ESET in July 2005 as the Director of Technical Education

MSAV 1.0

- Released March 1993 as part of MSDOS ® 6.0
- Included as one of many new utilities.
- Licensed and neutered version of CPAV
- Easily Attacked
- Poorly supported
- Short term impact to AV sales

MSAV – Take 2

- NOT another MSAV 1.0
- IS sold as a utility bundle
- IS sold and released with a beta component
  - Anti-virus
  - Firewall
  - Back up
  - File clean up
  - BETA, uncertified anti-spyware at retail price

Is OneCare Extortion?

Webster Dictionary, 1913 Extortion (Page: 529)

- **1.** The act of extorting; the act or practice of wresting anything from a person by force, by threats, or by any undue exercise of power; undue exaction; overcharge.
- **2.** (Law) The offense committed by an officer who corruptly claims and takes, as his fee, money, or other thing of value, that is not due, or more than is due, or before it is due.

Is OneCare Extortion?

Law.com Extortion n.

- obtaining money or property by threat to a victim's property or loved ones, intimidation, or false claim of a right (such as pretending to be an IRS agent). It is a felony in all states, except that a direct threat to harm the victim is usually treated as the crime of robbery. Blackmail is a form of extortion in which the threat is to expose embarrassing, damaging information to family, friends or the public.

Is OneCare Extortion?

- 1) Is Microsoft exacting payment from customers by threatening harm?

NO

- 2) Is Microsoft overcharging?

NO

Is OneCare Extortion?

NO!

It is extremely disappointing that some otherwise credible reporters have abandoned journalistic integrity, adopted a self-serving agenda, and stooped well below sub-tabloid standards in referring to Microsoft's re-entry into the anti-virus arena as "extortion".

That Said…

- MS often receives reports of vulnerabilities first
- MSAV team members participate in the evaluation of the vulnerabilities
- MS will need to be sure to share information as expediently as possible or it will look like MS is exacting payment for the earliest protection from OS/App vulnerabilities
- Delaying the sharing of information did not appear to be the case with the WMF or XML vulnerabilities

Some Outside Musings

- Nick Fitzgerald in an Alt.comp.virus post in 2003 addressed the rumor of MS entering the AV market and the “addictive update syndrome”

> *MS has never come close to this level or form of user "dedication", and may now see this as the route forward for increasing "revenue opportunities".*

Reported At VB 2005

- Matthew Braverman reports stats from the Malicious Software Removal Tool

Over the first six months, *Microsoft* recorded approximately 25 million downloads and 12 million executions of the tool via WU/AU. In other words, over 25 million unique computers were identified as being infected by Msblast, and the tool removed over 12 million of these infections.

Motives

- MS sees a way to help promote the adoption of security software
- MS also sees that more enticement than security is required, hence more than AV is bundled
- Some at MS think the big players in the AV industry are failing to innovate and need prodding.
- MS may be able to use AV to encourage patching

Motives

- The MS MSRT is locked into Windows update and hence cannot deliver timely protection
- MS may be able to deliver some protection via Windows Defender (included in Vista) outside of the “Patch Tuesday” constraints
- There is obviously a lucrative security market
- Protection of the Windows brand is a bigger financial motivation than AV revenues

More Musings…

- Jimmy Kuo responds to ZDNET article predicting the re-entry of MS in the AV industry

> *"consider that a warning"*
> *I'll consider it a warning when MS actually does it.*
> *Because that'll be two tries.*
> *And MS succeeds on its third try.*

- September 2006 Kuo leaves McAfee and joins MS

Symantec's John Thompson says…

"Our strategy is to out-innovate Microsoft. We know more about security than they ever will,"

Symantec threatens EU complaint against Microsoft

Sept 27, 2006 The Mercury News

Symantec to EU: Microsoft Trying To Shut Out Security Rivals

Sept 28, 2006 The Associated Press

Symantec says Vista will "reduce consumer choice"

Sept. 27, 2006 Ars Technica

Symantec Cries Foul over Windows Vista

Sept. 29, 2006 Sci-Tech Today.com

"Our strategy is to out-innovate Microsoft. We know more about security than they ever will,"

- This is a losing strategy for Symantec
- MS has experts every bit the equal of Symantec's
- If Symantec defines innovate as "acquire" MS is their equal
- Here is what Symantec and the rest of us are up against

Is OneCare Expedient?

- For MS - short term Ye$
- For Large AV companies – Short Term NO
- For the consumer – That depends upon quality
- For MS – long term depends on quality of support and the products

Quality of MSAV

- MSAV 1.0 had virtually no support – this is not likely to repeat itself
- MS support has made substantial progress in customer satisfaction
- MS has been building AV support experience since offering free anti-virus support in Oct. 2001
- MS TAMs are very respected support professionals
- Quality of service is a performance review metric

Quality of MSAV

- AV Built upon decent technology from GeCAD
- Researchers from GeCAD came to MS
- Further developed in-house
- Motivated developers, many with industry experience.
- MSRT proven robust and stable
- MS has never failed a VB test

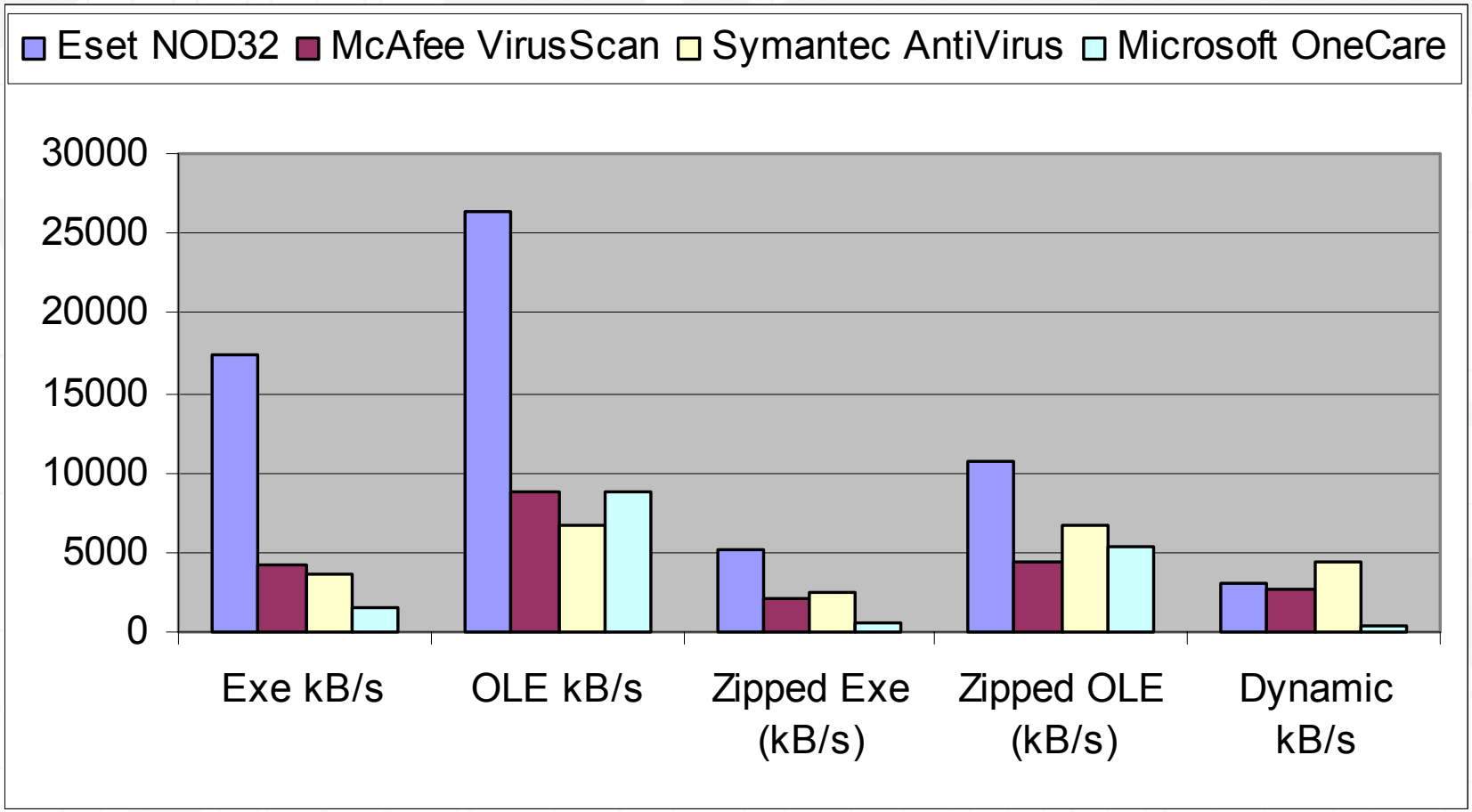
MSAV Performance

- AV-Test.org result in Blackhat presentation on runtime packed malware

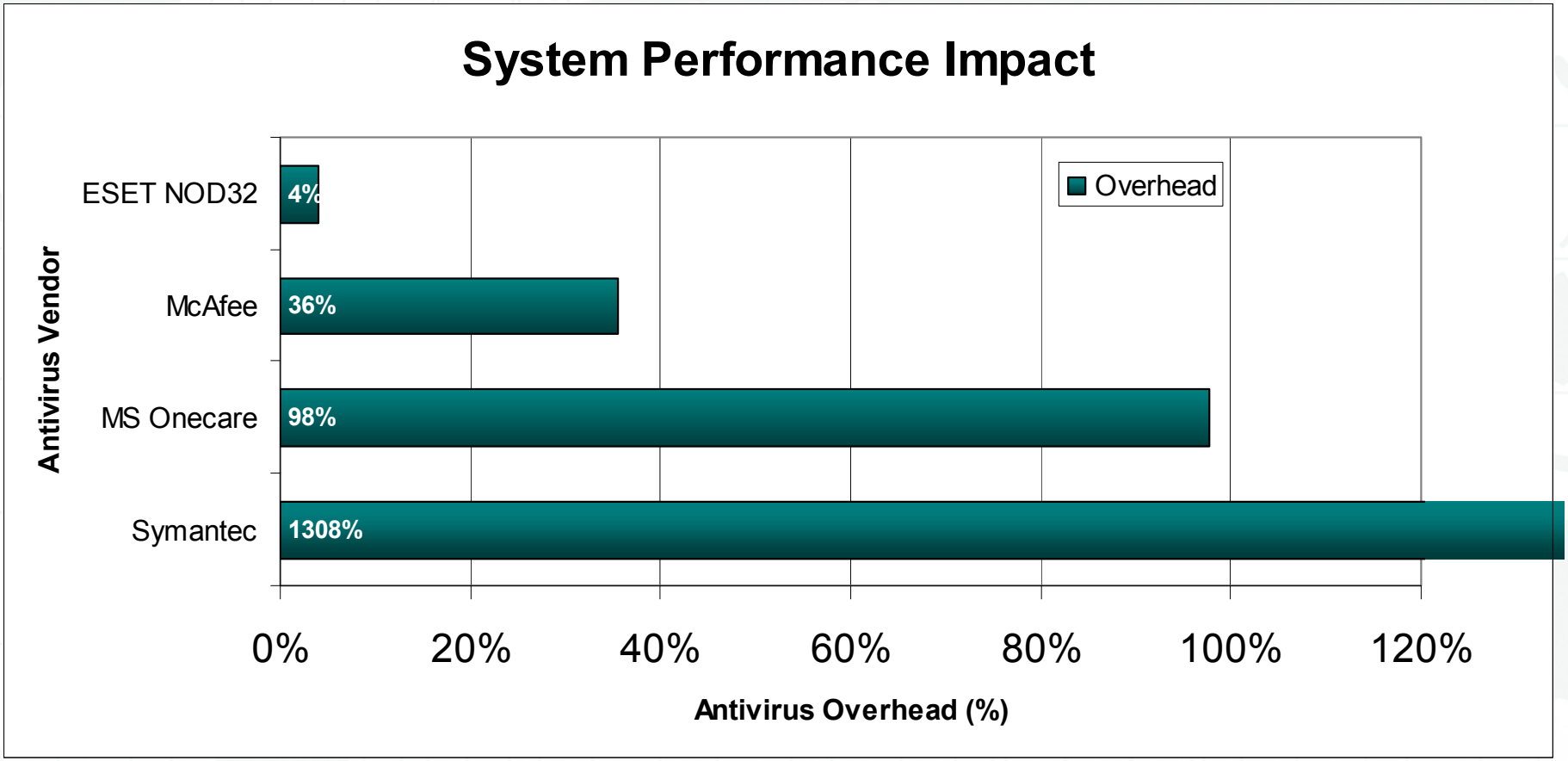
NOD32	82.83%
McAfee	79.39%
Symantec	58.62%
Microsoft	39.95%

MSAV Performance

- VB June 2006 Throughput



MSAV Performance



Quality of MSAV

- Currently sub-par AV protection
  - Late to detect WMF vulnerabilities Dec ‘05
  - Late to detect 0-day Excel vuln in June ’06
  - No perceptible heuristics
- Anti-Spyware is uncertified beta product
- Likely to improve… but why?

What will improve MSAV?

- Microsoft is motivated to protect the Windows brand
- Security is embraced by marketing more than ever before
- Employees are passionate about their work and self-motivated to produce quality software
- The Microsoft culture is conducive to excellence
- MS has a well funded research department

Quality not a given

- CA, McAfee, Symantec, and Trend also have deep pockets but have yet to deliver technically innovative products on a par with developers such as BitDefender, ESET, Kaspersky, or Norman
- MSAV will be the most attacked AV in the world

The Impact

- Ask Nick Fitzgerald if this is another “IE vs. Netscape Scenario”

And does MS really think it can (in the short term) take over enough of the AV industry to dominate? Remember, in the "browser wars" against Netscape, it was really two _emerging_ products fighting not only for market share but to shape the vision and direction of what that market was. Here we have MS swallowing up a small player in a very well- established sub-industry niche -- quite a different kettle of fish if you ask me...

The Impact

- MSAV is likely to impact large players the most
- OneCare will not be popular with “Best of Breed” buyers
- Customers of smaller vendors usually see through the marketing hype and buy for quality!!!
- There will be an impact and the pendulum is likely to swing both ways

The Impact

- OneCare is being marketed as convenience
- McAfee and Symantec have already taken a more comprehensive “Utilities” approach to compete
- Smaller companies may have to follow suit to maintain current growth rates

Hurdles

- Microsoft widely seen as writing insecure code
- When MSAV fails MS failed to protects the OS, not a 3rd party
- WGA Beta code distributed with WU
- Pro opt-out stance fuels SPAM problem

BIGGEST CHALLENGE

Have you ever tried to completely remove Norton Antivirus from a PC?

The 800 Pound Gorilla

The 800 pound gorilla is the dominant player in a market. For decades Boeing was the commercial aviation 800 pound gorilla. For operating systems, office suites, and Internet browsers Microsoft is the 800 pound gorilla. How does Microsoft's entry into the AV industry look to a small antivirus company?

NOD32 Vs. OneCare

- We already compete against the Symantec gorilla…

NOD32 Vs. OneCare

- We already compete against the McAfee gorilla…

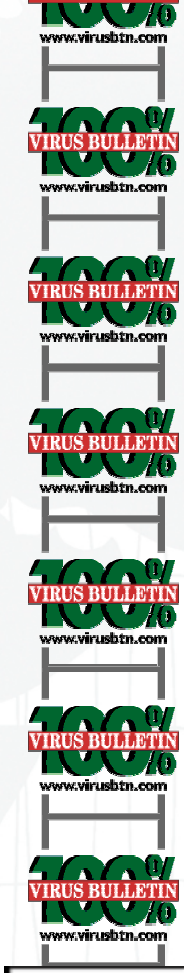
NOD32 Vs. OneCare

- We already compete against the Trend Micro gorilla…

NOD32 Vs. OneCare

- What's one more monkey in the zoo?

Setting the Bar




VIRUS BULLETIN
100%
www.virusbtn.com

VIRUS BULLETIN
100%
www.virusbtn.com

eset

ESET NOD32 Certifications

Record 40 Virus Bulletin 100% Awards

AV-Comparatives.org Advanced Plus

ISCA Anti-virus

Checkmark Antivirus 1

Checkmark Antivirus 2

Checkmark AntiSpyware (Desktop and Installed)

CheckVir Advanced

CheckVir MailScanner

So Microsoft, how high can you jump?

OneCare

To sum it up

- Microsoft AV is not extortion
- Microsoft AV is not expedient for the 800 pound gorillas
- Microsoft AV is currently not nearly as expedient for its customers as I believe it has the potential to be
- Microsoft AV will not be expedient for MS if it is adopted over superior products
- This is not the end of the industry

This is probably not the end!