

Samba On-Access Virus Scanning

Rainer Link
OpenAntiVirus.org
rainer@openantivirus.org

Agenda

- Introduction
- Reasons
- Concepts
- Considerations
- Pros and Cons
- Q&A

Introduction

- Interested in malware and anti-virus technology since 1991
- AMaViS developer from 1999 to 2003
- Co-Founder of OpenAntiVirus.org
- samba-vscan maintainer since 2001

Reasons

- Linux malware? nah, not really a threat
- Distribution of infected files via network shares
- Compliance (Basel II, Sarbanes-Oxley)
- Liability (e.g. KontraG [risk management])

Concepts

- Samba VFS
 - allows to „hook“ certain functions, e.g. file open
 - stackable since 3.0
 - allows to implement a wide range of (new) features
 - supports lots of OS (Linux, *BSD, Solaris ...)
- (Linux-) kernel based
 - syscall table hooking, VFS
 - limited OS support
 - allows to scan not only Samba shares (e.g. ftp incoming directory, NFS)

samba-vscan (I/II)

- Project started in Nov. 2001 with support for Sophos Anti-Virus („Sophie“) and Trend Micro („Sophie)
- currently 12 anti-virus products supported (requirement: must run as daemon; communication via socket)
- Samba 2.2.x / 3.0.x

samba-vscan (II/II)

- Features:
 - scan on open / close
 - file blocking (action: file delete, quarantine)
 - configurable limits (e.g. max file size)
 - exclusion from scanning via MIME-type or regular expression
 - file scan result caching
 - notification via Windows Messenger Service
 - Linux (x86, x86_64), FreeBSD (x86); Linux (PPC, IA64), Solaris
- Issues
 - messy code (e.g. lots of #ifdef)
 - too many global vars

other Samba VFS modules

- Kaspersky for Samba: scan result cache (via daemon), sources not easily available
- BitDefender for Samba: only a rather old version available, sources no longer available?
- F-Secure for Samba: discontinued
- Dr Web for Samba: sources available for download

Kernel-based

- open source
 - Dazuko: project sponsored by Avira, syscall table hooking (file close in 2.6 not available)
 - Fazuko: extended version of Dazuko, by F-Secure
 - RedirFS: project sponsored by Grisoft, VFS
 - Talpa: developed by Sophos, VFS, syscall table hooking
 - Kaspersky: syscall table hooking
- closed source
 - Trend Micro: syscall table hooking
 - CA: ?!
 - Symantec: ?!

Considerations

- virus scanning takes time
- virus scanning utilises (lot of) resources
- Samba 2.2.x/3.0.x supports only synchronized operations (scanning large ZIP on one share blocks all others)
- speed with Samba VFS / kernel-based scanning seems to be the same

Pros / Cons

- Samba VFS
 - limited to Samba (can't crash your whole system)
 - notification via Windows Messenger Server possible
- Kernel-based
 - not limited to Samba
 - no Win Messenger Service

Q&A

- Ask them now :)
- Hopefully some of questions will be answered as well in the upcoming comparative review paper on www.openantivirus.org