Demonstration of Operating Two Virus Scanning Daemons Simultaneously. VFindd and Clamd

The Leader In Total Security Solutions For
Linux, UNIX and Mac OS X

This document is a demonstration of operating VSTK-T with Clam-AV simultaneously on a Linux system.

The VFind Security Tool Kit Turbo edition daemon was specifically designed to not be interfered with or to interfere with the operating of other antivirus products that may be used simultaneously on the same system. Customers who experience any activity that might be considered interference are encouraged to contact CyberSoft for analysis and if needed correction.

The following example installs and operates the VFind daemon (VSTK-T Version 179) with Clam-AV daemon Version 0.97.3 simultaneously. The output of this report was from a live demonstration recorded using the script command. The output was formatted to fit the form of this document and to eliminate excess verbiage that did nothing to further the goal of the demonstration.

This first example is running the non-daemon version of clamscan as root against the /opt/vstk/bin directory which contains the VFind Security Tool Kit binaries. There are no false hits.

```
[root@jinhohost bin]# clamscan /opt/vstk/bin

LibClamAV Warning: **************************************************
LibClamAV Warning: ***  The virus database is older than 7 days!
LibClamAV Warning: ***   Please update it as soon as possible.
LibClamAV Warning: **************************************************

/opt/vstk/bin/avatar: OK
/opt/vstk/bin/vdlupdate: OK
/opt/vstk/bin/chashmerge: OK
.....
…. skip excess lines that do not demonstrate anything
.....
/opt/vstk/bin/miniweb: OK
/opt/vstk/bin/bhead: OK
/opt/vstk/bin/cronutil.sh: OK
/opt/vstk/bin/mergingVdl: OK
/opt/vstk/bin/vfecho_n: OK
/opt/vstk/bin/quarantine.sh: OK

----------- SCAN SUMMARY -----------
Known viruses: 1054224
Engine version: 0.97.3
Scanned directories: 1
Scanned files: 41
Infected files: 0
Data scanned: 0.14 MB
Data read: 0.07 MB (ratio 1.94:1)
Time: 6.581 sec (0 m 6 s)
```

This example is running the daemon version of clamd as root against the /opt/vstk/bin directory which contains the VFind Security Tool Kit binaries. There are no false hits.

Here we see that clamd is running in the process table.
[root@jinhohost bin]# ps -ef|grep clamd
clamav 17954 1 0 15:17 ? 00:00:00 clamd
root 17995 8906 0 15:21 pts/4 00:00:00 grep clamd

Here we run the clamd client program clamdscan against the /opt/vstk/bin directory with no false hits. This directory contains the VSTK-T binaries.
[root@jinhohost bin]# clamdscan /opt/vstk/bin
/opt/vstk/bin: OK

---------- SCAN SUMMARY ----------
Infected files: 0
Time: 0.130 sec (0 m 0 s)

This demonstrates running vfindd (VSTK-T) daemon at the same time that clamd is already running in the process table.

Start the VFindd daemon.
[root@jinhohost bin]# /opt/vstk/programs/vfindd-mt --threads=5 -4 --savepid=/opt/vstk/var/vfindd.pid

Run the vfindc client to provide the target files in the /opt/vstkbin directory to the vfindd daemon. IP protocol IPv4 is used by default. If you use IPv6 instead, please change ARGS in /opt/vstk/etc/rc.vfindd and the option for this script

[root@jinhohost bin]# find /opt/vstk/bin -type f -print|./vfindc

##==> VFind Client Version: 1, Release: 1, Patchlevel: 4 (April 2011)
##==> Do `vfindc --copyright' for copyright info.
##==> Do `vfindc --help' for help.
##==> Notice: Connected to 1 server at localhost
##==> Checking file: "/opt/vstk/bin/avatar"
##==> Checking file: "/opt/vstk/bin/chashmerge"
##==> Checking file: "/opt/vstk/bin/vdlupdate"
##==> Checking file: "/opt/vstk/bin/vdlupdate_Paul"
.....
…... skip *excess lines that do not demonstrate anything*
.....
##==> Checking file: "/opt/vstk/bin/miniweb"
##==> Checking file: "/opt/vstk/bin/bhead"
##==> Checking file: "/opt/vstk/bin/cronutil.sh"

##==> Checking file: "/opt/vstk/bin/mergingVdl"
##==> Checking file: "/opt/vstk/bin/vfecho_n"
##==> Checking file: "/opt/vstk/bin/quarantine.sh"

##==> Number of files read: 41
##==> No apparent virus infection found.
##==> VFind program termination

These tests were executed while both clamd and VFindd were running in the process table. There was no interference between the two products.

Additional Notes:

It should be noted that VFindd contains several API interfaces used for different purposes. The SVSP interface is the preferred API. Full documentation for the SVSP API with C language source code is contained on www.cybersoft.com. One of the multiple APIs available in VFindd is the Clamd antivirus API. The purpose of this API is to allow open source (or commercial products) which interface with Clamd to operate instead with VFindd without change.

In addition, it is noted that the entire Clam-AV signature system is a subset of the CyberSoft CVDL signature system. For those customers who need to make use of Clam-AV signatures simultaneously with CyberSoft CVDL signatures, that is possible. The Clam AV signatures would operate within VFind and would be available via all API interfaces.

In effect because VFindd is able to operate with the same API as clamd and because it is able to execute Clam signatures, it is possible to emulate clamd executing within VFindd either as a subset or alone. The advantage of this is that clients that need to conserve system resources or increase speed but need to operate two signature databases has this as an option.

If you are interested in this ability please contact CyberSoft to discuss. Finally, CyberSoft does not use or develop Clam-AV signatures and is not responsible for their accuracy. CyberSoft does develop, warranty and deliver CVDL signatures, which are copyright by CyberSoft.