Cybersoft.com

The World is at War in Cyber Space
We Can Protect Your Company
We Will Be The Last Man Standing

CyberSoft White Papers

VFIND, CIT: TAKE ON THE BARBARIANS ON THE OTHER SIDE OF THE WALL

By Roger Harmston

This article appeared in the SunServer monthly magazine, September 1996 Volume 10, Number 9 and appears here by permission of the author. Copyright 1996 by Roger Harmston.

This is a time for the good guys to finish first. The Bad Guys can be eradicated before they can establish a beach head.

The recently released General Accounting Office Report indicates that there are approximately 250,000 attacks on Government computers in the past year. And that number is doubling each year. One single documented attack cost more that $500,000.00 to repair (not including the value of the data lost).

Unknown is the undetected attacks.. and what they left behind. The actual numbers will never be known and statistics are scarce.

It can be a real problem to get good statistics about UNIX systems, since very few people report virus attacks and hardly anyone reports UNIX attacks.

I know of several customers who have found attacks on their systems using **VFind**, but they don't keep track of the problems, they just blow away the files and restore them from backup. Also, many people who are being attacked by software seem to think that they are having a hardware problem or that the system is corrupt, reformat and reinstall the operating system.

Earlier this year, at least one large international network of hundreds of UNIX on PC systems was knocked out of service by the Michelangelo virus. There are also indirect reports of the AT&T Attack Virus (portable shell script virus) eating UNIX systems in Europe.

There has been thousands of Trojan horse and bomb attacks (logic bomb and time bomb).

If you can believe it, at least one company sells a CD-ROM for $99.00 that contains the source code to the Internet Worm. Worm attacks are also common, but tend to be limited to bit-net based UNIX systems.

CyberSoft can't understand why the UNIX community continues to shove it's head in the sand when it comes to virus problems. It's as if the Typhoid Mary virus never happened, or that the Morris Worm didn't exist.

VFind was the first tool in a series created in 1988 when the creator, Peter Radatti, encountered a virus on a UNIX system. Over the years, it has evolved as a search tool for all forms of hostile software; but doesn't limit itself to viruses. The technical description should really be "a ***direct hostile algorithm examination and detection software package."***

VFind is totally unobtrusive and unencumbered by Graphical Interfaces. For a very good reason. It's impossible to design anything non-intrusive if there has to be a user GUI interface with user interaction.

Run as a cron job, the only time you hear from it, is when there is a problem. A series of example scripts are included to get you up and running immediately and serve as models for your own scripts.

It would be a nightmare attempting to constantly be doing new routines to search for something new. As a result CyberSoft developed **CVDL** (CyberSoft Virus Description Language).

CyberSoft is constantly doing new routines to search for new things. The **CVDL** helps a great deal since we can write a generic model for something like a recursive bin remove and that one model will catch millions of actual versions.

An important component is **CIT** (Cryptographic Integrity Tool). By incorporating MD5 hashing algorithms, **CIT** can locate any file that has been modified, deleted or added to the system by outsiders, viruses or any other form of attack. This tool is extremely fast and will assist an administrator in finding the problem within minutes. Your personal creativity will undoubtedly come up with thousands of uses for **CIT**. Anywhere that it is important to prove that data or any combination of data has been unchanged from it's original state will be a prime candidate for **CIT**. **CIT** can be used across network boundaries (including the Internet), post office, or ANY form of transmission to be absolutely sure that data integrity is preserved.

I used **CIT** to verify versions of my software archives against what was on the system. Instead of laboriously checking dates, file sizes and naming conventions (and still not being absolutely sure), I was able to quickly (within 5 minutes) compare more than 11,000 files. The limiting factor was the speed of the 4 MM. DAT drive NOT the application.

CIT ships with **VFind** but can be purchased separately if required and works on Solaris and other UNIX platforms, NT and DOS.

THD is a Trojan Horse Detector. This a useful tool to detect Trojan files that are unwanted or potentially harmful to your system. If matches are found when comparing files against a data base file; reports are generated to alert administrators to altered files.

See the CyberSoft Home page at ***http://www.cyber.com***. for the white papers. They are full of extremely useful hints and valuable information.

Don't get caught. Viruses and Virus programmers are getting very sophisticated. Complacency will almost certainly guarantee that you will get nailed. Have the tools in place to prevent an attacker from getting a foothold on your system.

As Kane and Roberts state in ***Computer Security***, "the ultimate responsibility for protection of yourself and your property rests with you".

Readers of my Solaris Column will know how paranoid I am about security for our customers. Peter Radatti and CyberSoft are an answer to my prayers. They understand the problem and have set about to deliver a suite of products that ensure the integrity of my site. **VFind** and **CIT** are very inexpensive tools that can save your company huge amounts of money in tracking and eradicating problems.

This is the first time that I have ever give and A+ for implementation of Vision in my score card when evaluating products. This is elegant execution of an extremely complex series of tasks.

Roger Harmstron is with Strategic Unix Networks Corp. in Victoria, British Columbia. He can be reached at roger.harmstron@strategic.Victoria.BC.CA

Product Evaluation Score Card

Company:

CyberSoft Inc.
1508 Butler Pike
Conshohocken, Pennsylvania 19428
Phone: +1.610.825.4748
FAX: + 1.610.825.6785
Email: info@cyber.com
Web: www.cyber.com
Product: VFind, CIT

Corporate Vision

Implementation of Vision: A+

Response

Email Response: A
Phone Response: A

Marketing Depot Response: C+
Help Desk Response: C
Web Page: A
White Papers Available: A

Documentation

Quality: C+
Content: B+

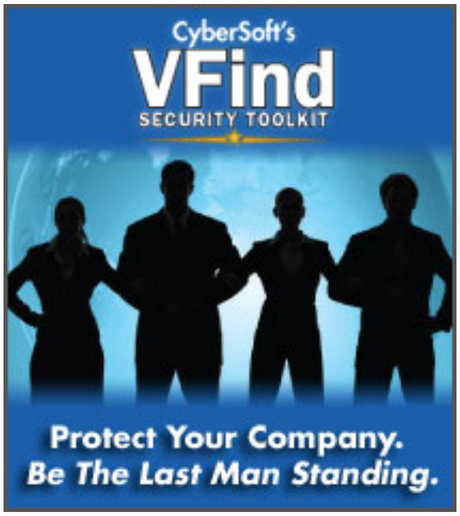
Multi Platform Interoperability

Ease of use: A
Ease of integration: A
Installation: B+
Grade Average: B++

Key to Grades

Mark	Rate
A Excellent	7
B+	6
B	5
B-	4
C+	3
C Acceptable	2
C- Barely Acceptable	1
F - Fail	0

AhnLab
V3 Internet Security 8.0
Fastest and Lightest
All-in-One Security Solution
Exclusively imported and supported in the United States and Canada by CyberSoft Operating Corporation



This site certified 508 Compliant