INTERHACK

Interhack
2599 E Main St #512
Columbus, OH 43209

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

Spector Professional Review and Commentary

Matt Curtin

May 7, 2002

1 Introduction

Spectorsoft Corp. publishes a product known as Spector Professional Edition for Windows. It's advertised as "Internet Monitoring and Surveillance" software, which is more commonly known as "Spyware".

A quick look at Spector Pro revealed several key issues:

- The software's "stealth mode" is sufficiently obfuscated that typical users will have no idea that the software is active.
- Because the software runs on the user's computer itself, the computer cannot be trusted. Any attempts to determine what is happening while the system is booted and running normally can be foiled by the software.
- The software requires network connectivity to operate. This means that watching online activity from a trusted machine (including firewalls, proxies, and network intrusion detection systems) will yield evidence of Spector Pro being in use.

The bottom line is Spector Pro can completely compromise the privacy of a non-technical user. Competent professionals looking for Spector Pro's presence should have no difficulty finding the software.

2 Detailed Discussion

A cursory examination of a Windows 2000 Professional workstation with Spector Pro 3.1 confirmed some claims of the software and yielded some fairly interesting discoveries.

2.1 Stealth Mode Effectiveness

Effectiveness of the system's Stealth Mode depends on obfuscation. Users who do not know what processes to expect on a process listing, or believe that programs must be "visible" to be running, stand no chance of determining that Spector Pro is active. No indication of Spector Pro (or Spectorsoft) is found in the process listing, host registry, or visible files.

A particular key combination (apparently "Control-Alt-Shift-S" by default) on the keyboard will bring up Spector Pro's splash screen and a password dialog box. A user who happens across the correct key combination would find that the software is running.

The ability for Spector Pro to hide is dependent upon its running. If the disk on which it is installed is examined with another operating system, for example, files invisible to Windows users would be clearly visible, though perhaps still not obviously named.

2.2 Exploits Lack of Trusted Computing Base

Information security practitioners have long used the concept of a Trusted Computing Base (TCB) to define the collection of components used to enforce a security policy. The TCB's ability to enforce policy depends on the correctness of implementation. Windows operating systems largely fail to adhere to sound security design principles. Furthermore, the complete lack of trustworthy audit mechanisms makes it impossible to verify in any reasonably secure manner what is and isn't happening on the machine.

Spector Pro takes advantage of this lack of security in Windows, effectively turning what should be the TCB against the user, recording his activity and making it impossible for him to audit the computer's activity.

For this reason, examination of a machine with Spector Pro enabled is best done not with the machine booted normally, but by looking at the disk under another operating system that will not be running the Spector Pro software.

2.3 Spector Pro Requires Network Connectivity

Interestingly, Spector Pro will require network connectivity for it to operate. Alerts that it sends to the person monitoring the system's use, as well as other data regarding the activity, are routed through Spectorsoft. As is true with the rest of the system, the network activity is heavily obfuscated.

2.3.1 Uploads to Spectorsoft

In our quick assessment, we identified that even without specifying an address to which alerts should be directed, Spector Pro was uploading data to Spectorsoft.

We found that among the normal network traffic, our test machine was making TCP connections to the host u2a1376gf-43ty-245b.com [209.61.191.54]. The domain in question is registered to none other than Spectorsoft.

```
SpectorSoft Corp. (U2A1376GF43TY245B-DOM)
   333 17TH ST
   VERO BEACH, FL 32960-5670
   US

   Domain Name: U2A1376GF-43TY-245B.COM
```

Clearly, use of the domain U2A1376GF-43TY-245B.COM is simply an obfuscation technique, hoping to foil the casual observer.

2.3.2 Obfuscated Sessions

In addition to obfuscation in the domain name, Spector Pro uses an obfuscated binary protocol for the interaction with Spectorsoft. Figure 1 shows the data, in hexadecimal form, that are uploaded to Spectorsoft.

```
00000000  01 00 00 00 0c 01 00 00  00 00 02 00 44 4c 61 33
00000010  bd bd 3a 8d bc ce bf fd  84 ce 37 05 6f bb 95 25
00000020  9c 33 57 0e f7 6d 91 60  f5 d0 f2 f9 70 99 cf 97
00000030  21 24 69 04 5b 84 32 74  66 55 5c 04 66 83 71 84
00000040  b9 8f 10 bf da f1 26 61  f7 c9 3f 60 bc f2 45 f6
00000050  18 d9 e6 82 27 37 38 a4  14 ed bb 2e c7 19 4e ff
00000060  f6 b3 fe c3 54 7d 03 6f  67 51 3f a8 65 ee bf 0c
00000070  e8 5a a0 ae a3 8e 98 26  5f 6c 3b 76 ae f8 57 49
00000080  74 33 c7 c3 c2 0c 50 aa  5f 0d 17 2a fe b7 d9 b8
00000090  de 23 c8 26 41 d0 c6 19  41 17 44 72 15 70 33 8b
000000A0  47 3a a1 aa 04 92 70 c2  6c 94 af 71 ed 9d 4e f7
000000B0  14 da 6f 2a 47 ff 8a 97  80 11 d0 e8 18 bb 9f 70
000000C0  0a cc f7 ce 11 58 31 c7  43 dc d2 25 99 63 bb e0
000000D0  7e 4f d1 c0 3e fc 50 c8  1d 4a e1 0d 3f 70 e4 4b
000000E0  e0 c1 36 e8 c2 14 88 5c  2b 6e fa 22 19 3d 8d 3f
000000F0  a0 1f 1a 66 94 e5 fc 73  47 ca b7 a7 11 38 4b fc
00000100  93 af 29 96 10 1b 03 6a  2a fd e5 20
```

Figure 1: Initial Message to Spectorsoft

Additional data are in the session after the initial message from client to server. Further, toward the end of the session, the message length becomes significantly shorter, suggesting that there is some kind of interactive protocol, rather than simple data uploads and downloads.

The end result is that neither the user of the machine being monitored nor the person who installed the software can be sure of just what is being uploaded to Spectorsoft. Furthermore, in our test, there was no obvious need for Spector Pro to communicate with Spectorsoft, which suggests that there is more to the communication channel than what's needed to provide the "alert" functionality.

So the question is, "Does Spectorsoft spy on the spies who use Spector Pro?"

2.3.3 Network-Based Defense Mechanisms

Because Spector Pro requires network connectivity to perform its work, network connectivity is its Achilles' Heel. Several technologies could be employed to detect the presence of Spector Pro.

Network Intrusion Detection Systems These systems could simply be on the lookout for connectivity from their client machines to TCP port 16771. Additionally, they could be on the lookout for DNS queries for the zone U2A1376GF-43TY-245B.COM.

Application-Layer Firewalls Because these systems will not be able to pass traffic for protocols they do not understand, application-layer firewalls will prevent Spector Pro from operating correctly. (We have not investigated whether Spector Pro can work with firewalls, which it could do by encapsulating the data in HTTP requests. If it does, however, such firewalls could be configured to look for connections to the obfuscated hostname.)

3 Conclusions

Quick assessment of Spector Pro shows that it is effective spyware, giving typical non-technical users little chance to protect their privacy. As with all such technology, however, this is essentially an arms race. Once users become more sophisticated, perhaps by employing some techniques described here, they will regain the upper hand. Such a shift in the balance will no doubt result in greater obfuscation in Spector Pro, which will result in greater sophistication of privacy-sensitive users. Whoever has the greatest invested, as a combination of skill and time, will win, until someone invests more.

Ethical considerations here are myriad. Besides the basic questions of who may spy on whom and for what purposes, a basic issue comes into play with regard to the technique employed. Namely, this technique requires that some data, which are obfuscated and therefore difficult or impossible to audit, are uploaded to Spectorsoft. Email alerts are routed through Spectorsoft.

Parents that monitor their children's activity with this software will also be giving Spectorsoft a clear view of what their children are doing. Employers that monitor their employees with this software will also be giving Spectorsoft a clear view of what their employees are doing. Proprietary and otherwise sensitive data are certain to fall into Spectorsoft's hands. We thus raise the question, "Who is Spectorsoft, and why should you trust them to keep your secrets?"

4 Acknowledgments

Paul Graves of Interhack was instrumental in the completion of this analysis. Roger McCoy of WBNS-10TV (Columbus, Ohio) provided the impetus for this investigation and commentary.