

Spectrum Countermeasures

5617 133rd Street Court, Apple Valley, MN. 55124 (952) 431-5821

*Tom -
For your review.
Stuart
12/10/03*

December 10, 2003

~~Stuart R. Romenesko
Petters Group Worldwide, LLC
4400 Baker Road, Suite 200
Minnetonka, MN 55343~~

Dear Mr. Romenesko:

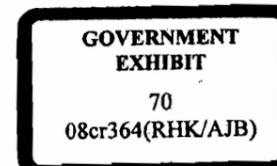
Thank you for the opportunity to conduct a countermeasures sweep for Petters Group on December 6th. I have enclosed my report on the results of the sweep. If you have any questions, please contact me. I have also enclosed my statement for the work performed.

Please let me know when you would like to start the Level B sweeps that we discussed. I will be out of town from December 12 to December 22. Thank you.

Yours truly,



Steve Russell



0070.0001

**Technical Surveillance
Countermeasures Survey**

December 6, 2003

Confidential

0070.0002

Objectives and Procedures

On December 6, 2003 Steve Russell conducted an electronic sweep of the offices of the Petters Group, 4400 Baker Road, Minnetonka, Minnesota, at the request of Stuart Romenesko. Russell was assisted by Bill Kimberly, and was observed by Shawn Monighan, of Petters Group. The purpose of the sweep was to determine if any electronic eavesdropping devices were in place in the designated offices and rooms.

A thorough physical search was made of each room. This included removal of outlet and switch covers, physical examination of telephones, and a search of ceiling areas, including suspended ceilings. In addition, a short-range broadband detector sweep with coverage up to 4.5 Gigahertz was used in the physical inspection process.

Audio sources were placed within each office to activate possible voice-operated bugs and to provide continuous audio output from unoccupied rooms. The radio frequency spectrum from 25 MHz to 1300 MHz was searched manually with a specialized communications receiver. All anomalies were noted for future comparisons. No audio was detected on any of these signals.

The following offices and rooms examined:

Patty Hamm office
Deanna Munson office
R. White office
Stuart Romenesko office
Tom Hay office
Ted Deikel office
Tom Petters office
Mary Pernula office
Executive area conference room
Vacant office directly across the hall from the executive offices

0070.0003

Board room

Large storage room across from Munson office

Telephone wiring, wiring closets, and the Intertel Axxess 1024 telephone switch were examined.

The digital telephone switch employed by Petters Group, an Intertel Axxess 1024, is an effective preventative measure in avoiding electronic wiretaps in itself. All but the most sophisticated penetration attempts would fail. Only the federal government currently has the resources and technology required to directly penetrate such a system. However, there are approximately 80 analog lines, which are used for applications such as modems, facsimile, cordless phones, and the Polycom conference phones. These are always a concern as audio can be more easily directed out of the building on these lines.

While examining the telephone closet just outside the executive spaces, non standard wiring and hookup were found which appeared to be suspicious. We requested Shawn Monighan to help us determine the target and source of the wiring. The wiring was not completely explained, but we are satisfied, based on Shawn's investigation, that it was not an attempt at electronic eavesdropping. As part of the record, his email to Steve Russell is attached below, in its entirety.

"Here is my follow up on the phone item that we found on Saturday.

In the 2C closet, there was a hanging cross-connect wire going from the feed panel side (goes back to switch room) on punch down 2C-084. The other end of the hanging wiring was punched down on the wire that goes to jack 2C-112. Jack 2C-112 is the jack that Sandy Indahl's phone (Ext 14827) is plugged in to.

After some research, I determined that there is no 2C-112 punch down on the feed panel side in the 2C closet. This means that when the building was originally wired, the person pulling feeds back to the switch room did not include enough feeds to match the number of jacks that were being wired.

0070,0004

So here is my theory as to why the loose wire was there. I know it has not always been there. I think it is relatively new.

1) My theory is that when we moved in to the building in Sept 2002, Inter-Tel patched Sandy's phone in the 2C closet by going from the 2C-112 punch down to the 2C-084 feed punch down. This worked fine and was no problem. I know it was punched down with a nice tight clean cable because I never noticed the hanging cable before.

2) In the recent months, Inter-Tel probably discovered that this particular wire was going from 2c-112 to 2c-084 and pulled the wire so that they could correctly punch it down. After they pulled the wire, they discovered the lack of 2C-112 feed back to the switch room. They couldn't find any new wire in the closet so they reused the wire that they just pulled but it was not long enough to wrap cleanly around so they left it hanging for us to fix when we got more wire in the closet.

This morning, I put a new roll of new wire in the 2C closet and recross-connected Sandy's phone with a nice clean and tight wire."

End of Shawn Monighan email.

Conclusion

Our conclusion, based on the physical search, radio frequency spectrum search, and examination of the telephone system, is that there are currently no electronic eavesdropping devices within the area searched. While we cannot guarantee that there have not been any devices in the past, we found no evidence of any.

General Security issues

There were several security items that could, or should be addressed:

- In the executive suite reception area there is a coat closet in which is located a key cabinet. The cabinet was unlocked and there were a number of keys, including keys to Mr. Deikel's office and desk. Having a hidden key cabinet like this is a good idea, but it becomes a liability when it is not locked. A small safe, built into the wall, with a digital combination could be used for that purpose.
- In the office of Deanna Munson there is a safe which is clearly visible from the window. This might prove to be a temptation to the criminal element, or to teenagers looking for an opportunity. Moving the safe to a location not visible from the window, or concealing it within or behind another object would eliminate this temptation.
- In the large storage room across from Munson's office, there are unused phone jacks and coiled up telephone wire in the ceiling. Unused wiring should always be removed as these can easily be used to run microphone audio from the room to another place in the building, or to a transmitter.
- There are several Polycom speaker phones throughout the office spaces, used for voice conferencing. These are analog devices, as opposed to the normal digital telephones you have. As such, they are vulnerable to taps and should be checked for those periodically.
- In the telephone wiring closet just outside the executive spaces, which is used by janitorial personnel, there is a wiring cabinet that is made of thin wood, and is not locked. That should be corrected. Ideally, there should be a metal door and it should be locked. This was pointed out to Shawn Monighan.

0070.0006

- Within that cabinet, we discovered a pair of wires coming off PBX to JK 2C084 at JK 2C84, which is connected in the ground floor closet to jack 2C112. The wiring was not in accordance with the other wiring in the cabinet, and is suspicious.
- There were various combinations of unlocked office doors, unlocked desks and cabinets. which may, or may not be of concern to you.
- There were a couple instances of information left on dry easel wall boards, which may, or may not be of concern to you.
- It appeared there were a number of paper shredders in these offices. Assuming they are used regularly, this enhances your information security.

Prevention Considerations

There are numerous motives for electronic eavesdropping. Centers of power, business, technology, and finance will always be attractive targets for electronic surveillance. A large company such as Petters Group, would certainly qualify for such interest. Additionally, internal activities and politics are sometimes motivating factors for electronic spying.

Devices can be brought in by people doing work in the building, such as janitorial, catering, or maintenance. In addition, it is certainly possible that even a trusted employee may be compromised and be used to plant a device. Such devices may be designed to be left in place, or in some cases may be removed immediately after an important meeting.

Protection against such devices can be divided between prevention and detection. Prevention techniques would include careful monitoring of maintenance and janitorial personnel. Alerting employees to the risk is also important. Detection would include physical searches and RF sweeps.

The FBI, for example, assigns a clerical employee to escort all maintenance personnel. They are supposed to watch all their activities while in secured spaces. In real life, after a few minutes the employee becomes bored and pulls up a chair and pulls out a paperback. It is difficult to motivate individuals to observe with enough diligence to really make a difference. Realistically, someone working in a ceiling could still easily plant a device and never be observed by a monitor.

We suggest that all maintenance personnel are logged in, with notation as to their name, company, date, time, reason for the work, specific location of the work performed, and the time they left. With such information, someone conducting a sweep can quickly conduct a physical search of the area where the work was

done. If the log is accurate there is really not much need to tie up an employee to observe the maintenance personnel. Of course, if the work is performed through a large room or large area then the physical search will also require more time.

Janitorial personnel present more of a problem. They are usually working at hours when there are few other people around, and they usually have access to most of the office space. The FBI addresses this problem by conducting background investigations on all janitorial personnel and by conducting frequent sweeps.

It is a fact that the main source of information leaks is one person talking to another. It is human nature to want to feel important or knowledgeable. Knowledge is power and telling secrets sometimes make people feel good. Sometimes these slips of the lip are deliberate, sometimes innocent, and accidental. However, unless you have unusual employees, not susceptible to human frailties, you will have leaks. If you have an opportunity to talk about security with these personnel, it could pay dividends to remind them about these issues. They are probably aware of the risk of bugs and one might suggest they conduct a brief inspection of their office, perhaps on a weekly basis. They should be warned of the risks of accepting gifts, such as plants, or office decorations designed to be kept in the office environment. Bugs can be built into most of these items, and can function for long periods of time with adequate batteries. These bugs could be monitored from within the building, or adjoining buildings. The walls of your building present no impediment to radio waves.

This report was compiled by Steve Russell
December 9, 2003

0070.0009