

Date: June 21st, 2004

Subject: Grievance

Title: Privacy and security concerns related to the use of 'keystroke logging' surveillance software at Parkland Regional Library.

Comments: It is with careful consideration that I am asking this grievance be considered if for nothing more than a simple review of recent events and the privacy and security concerns relating to these events. For the sake of expediency I am keeping the details brief without consciously limiting the impact of the message I hope to relate.

On Thursday, June 17th I was performing routine maintenance on my workstation when I discovered the presence of a 'keystroke logger' on my computer. As a trained computer professional my immediate reaction was to remove this insidious blight and ask questions later. The prudent next step would be to try and determine where it came from and whether or not it had been used for nefarious reasons. This is exactly how I responded but in retrospect I'm not so certain this was the correct course of action. I should have immediately requested that any computers suspected of containing information be secured and audited for any abnormalities or forensic evidence.

First thing I did was locate the folder that had spawned this 'trojan' to see if there was any evidence pointing to where it had originated. A cursory look through the "c:\Program Files\STARR\" folder showed that it had been installed on May 20th, 2004 but little else. A quick look in my day timer also indicated that I had been at the Olds Library on May 20th and had arrived back to PRL at approximately 3:00 PM. There was also a small note in my day timer with the following, "VC logged into my comp???" Upon reading this I recalled that on May 20th after returning to PRL I had been unsuccessful in logging in to my computer for the first couple of tries. A closer look revealed that user "vclev" had been the last one logged into my computer and that user name was the one I had been trying to login as, but using my password.

I did a quick search on Google for a 'removal tool' and went about securing my workstation. Once that was accomplished I did a quick check on the Windows 2000 server to see if it too had been compromised by a 'keystroke logger'. First thing I noticed was a folder named "STARR" spelled exactly the same as the folder I had discovered on my workstation. A quick look in the folder revealed half a dozen or so files and one or two sub-folders. I noticed that the file names contained computer names with user names appended after an underscore. The two computer names were PRL16 which I recognized as my workstation and the other one was called NET something. The three user names that I remember seeing were "Administrator", "darme" and "vclev". At this point I decided that I had seen enough and had better check the running processes to see if it included a file named "wsys.exe" as this was the 'keystroke logging' program that I had discovered on my workstation. I observed that it didn't.

At this point I pushed my chair away from the keyboard and tried to decide what my next move should be. My first decision was to not do any more investigation as it could possibly disturb any potential forensic evidence. Needless to say, there were a lot of unanswered questions and I was unsure how to proceed. Not only was this a major privacy concern it was also a major security concern. I knew my on-line banking account and PIN number had been compromised as I had logged in to my account only a few days before but it didn't make any sense to login and change it because as far I was concerned the whole PRL Network was a 'red zone'.

The first thing I did upon my return home that evening was to check for the surreptitious installation of any rogue programs on my personal computers and then change all my passwords. I then related the day's events to my family and we sat down to discuss the implications of all this. Here is a partial list of the questions we didn't have a definite answer on:

- Who had installed the "keystroke logging" software?
- Had more than one person been involved?
- Was this authorized?
- Why was it installed?
- How was the information that was logged being stored?
- Had any of the information been used for nefarious purposes?
- Was this even legal?
- Was this surveillance conducted across the board or 'targeted'?

On Friday morning it soon became evident that my immediate supervisor, Michael Silver had discovered the 'keystroke logging' software had been removed from my computer. He started off with a series of 'probing' questions that I tried to avoid and before too long he asked if the security concerns I was referring to were in any way related to "Starr". I told it was and he indicated to me that it had been approved by the board of directors. I indicated that I thought it was a tad intrusive, invasive, and excessive and his response was that it was used on a 'rotating' basis.

I told Michael Silver that in light of the fact that I had asked for and received permission to use my work computer to do on-line banking and that he subsequently installed a 'keystroke logger' on the same computer therefore compromising my account number and PIN it left me with no alternative but to lodge a formal grievance. He then said that the first step would be to discuss it with my supervisor and demanded that I follow him to Patricia Silver's office. I told him that my interpretation of the 'Grievance Procedure' was that I take it up with the Director and that if I felt it hadn't been properly addressed at that level then I should escalate it to the next level, that being the Personnel Committee. I also told him that under the circumstances I didn't think it was appropriate to continue the conversation with him as it affected him directly but he would hear nothing of it and we ended up in Patricia Silver's office with Donna Williams sitting in as an observer. At this point I was thankful to have a neutral party present as I felt I was being badgered. Even with Donna Williams present Michael Silver gave me little opportunity to provide any input and when I attempted to correct him on a couple of points I was summarily cut off.

Towards the end of the meeting I sensed that Donna Williams was unaware of the nature of 'keystroke logging' software or its huge potential for abuse. She did not seem to be aware that this software was one of the few things that could compromise a password and even render encryption moot as the damage would be done before the data even had a chance to be encrypted.

It should be noted that it is unlikely the computer where the 'keystrokes' have been logged is secure and, should it be compromised the passwords for all the servers at Parkland Regional Library would be sitting in clear view in a text file along with all my banking information. Not only does the use of 'keystroke logging' software raise all sorts of serious privacy concerns its misuse represents a huge security problem. Just think for a minute how this information could be used to discredit my integrity or for other fraudulent or nefarious purposes. I somehow can't help but think that the Board of Directors was somewhat misled as to the nature of this software, what it was supposed to accomplish and the liability concerns it presents when they took the risky step of approving it.

Conclusion: Firstly, as should be evident by now, there are complicated and far reaching privacy concerns in respect to the use of this category of software. If 'performance monitoring' was the intended purpose then I would suggest that there are many tools available that are, for one thing free, and for another are better suited to the purpose without the huge liability potential. Furthermore, without a clearly defined policy laid out for the use of 'keyloggers' or a multi-tiered authorization procedure the potential for abuse is just too huge to ignore.

Secondly there are the security concerns associated to the misuse of 'keyloggers'. Most software in this category tends to save the results in nothing but plain text files in an unsecured folders likely sitting on Microsoft Windows computers that are trivial to compromise unless a concerted and tedious hardening of the operating system and it's authentication process is performed. By using a 'keylogger' the security issues begin cascading.

Thirdly, is the information gathered really that useful? I would say not. I'm sure that the first line of defense for anyone entrapped by a 'keylogger' would be to claim that because the passwords have been compromised there is little to prevent someone from logging in to the infected computer as the intended victim and performing all manner of mischief. Without any accountability who could argue otherwise? Without any accountability just imagine the potential liability.

Another thing that comes to mind is if consideration was ever given to less invasive, intrusive, and excessive performance monitoring? Log files can offer any information necessary in this respect. If misuse of resources is an issue then was consideration ever given to locking down the workstations and only providing the applications that were necessary to perform the work required. Solutions like these present a significantly smaller liability threat than something as sinister as a 'keylogger'.

I fear that the manner of which these events have unfolded has left an opportunity for the deliberate destruction of any potentially incriminating evidence. In fact, if the 'STARR' folder has been removed from the Windows 2000 Server I would have to concluded it was performed in an effort to conceal the identity of any possible perpetrators, their accomplices or otherwise potentially incriminating evidence.

As I am in no way or form an expert in legal matters and as I have had little time to prepare this I would ask that this document be left open for amendment or correction and that it be parsed by a legal expert for any any omissions or inconsistencies of a legal nature.

- Suggestions:**
- Consider less risky alternatives to performance monitoring.
 - Draft a clearly defined procedure for the deployment of this category of software and have it reviewed by a legal expert.
 - Consider a multi-tiered authorization mechanism before deploying this category of software.
 - Notify personnel that they could be under surveillance at any given time although I would be hesitant to deploy any surveillance at all as it has been shown to lower moral and can easily have the opposite effect from it's intended objective.
 - Consider the use of this category of software only under certainty that crime or fraud is suspected. Even then I would be careful with it's deployment.

- Requests:**
- I would ask that this unsolicited collection of my personal and private information be secured by an impartial third party and audited for any evidence of alteration or nefarious use.
 - I would ask that any unsolicited collection of personal and private information be exempt from any performance review.
 - I would ask that the use of 'targeted surveillance' be terminated until a complete review has been completed by the Personnel Committee or an equivalent authority.
 - I would ask that I be provided with written assurance that I be exempt from any liability in respect to the compromised passwords and sensitive information collected without my knowledge or agreement.
 - I would ask that I be provided with expert legal assistance before any action is taken in respect to this grievance.

Dated and signed this 21st day of June in the year 2004 in the Town of Lacombe and the Province of Alberta.

Complainant: Dan W. Armeneau _____

Director: Patricia Silver _____

Witness: (_____) _____