The Ear of Sauron

In The Lord of the Rings, Sauron wiles away the time peering out over Middle Earth with the Eye – lacking Internet access, Sauron couldn't occupy himself flaming hobbits online.

What you will learn…

- A future direction for spyware
- How stolen audio data can be exploited

What you should know…

- What a botnet, botmaster, and zombie are

Sauron's Eye has been realized, in a small way, by the webcams perched atop our monitors and embedded into our laptops and mobile devices. The presence of webcams has not gone unnoticed by spyware, and there have already been a number of cases where people were caught peeking (GuardiaCivil05, Kambas08, Leyden05, Voyles08).

What of the other senses? Computers are not commonly equipped with USB noses and tactile devices (much to the chagrin of perfume manufacturers and porn studios, one imagines), but they do often have microphones. Microphones are now standard equipment on laptops, and they started appearing on desktop computers twenty years ago, in 1990 (OGrady08). This was undoubtedly inspired by the fantasy of controlling the computer by voice commands, being years before VoIP hit the market. Needless to say, the microphones were put to good use.

In fact, I recall working as a system administrator in the early 1990s, when a user sheepishly poked her head into my office and said *John... the computer is talking to me*. I found, upon investigation, that someone had installed a program on her Mac called *Conan the Librarian*. *Conan* would monitor the microphone, responding to the first burst of noise by saying *quiet* and then *quiet!* and becoming progressively louder and more insistent with each sound until *Conan* was screaming *QUIET! QUIET!* at a hapless user. (For the hapless user in this case, I solved the problem by turning the microphone to face away from her; not every technical problem requires a technical solution.)

Conan was an early example of a program spying on a user using the microphone, albeit without malicious intent. We do object to people and programs spying on us, in general, and so physical indicators appear to warn us: the sound when a cameraphone picture is taken, the light beside webcams. Microphones have no such indicator, though, and can easily be enabled surreptitiously by spyware.

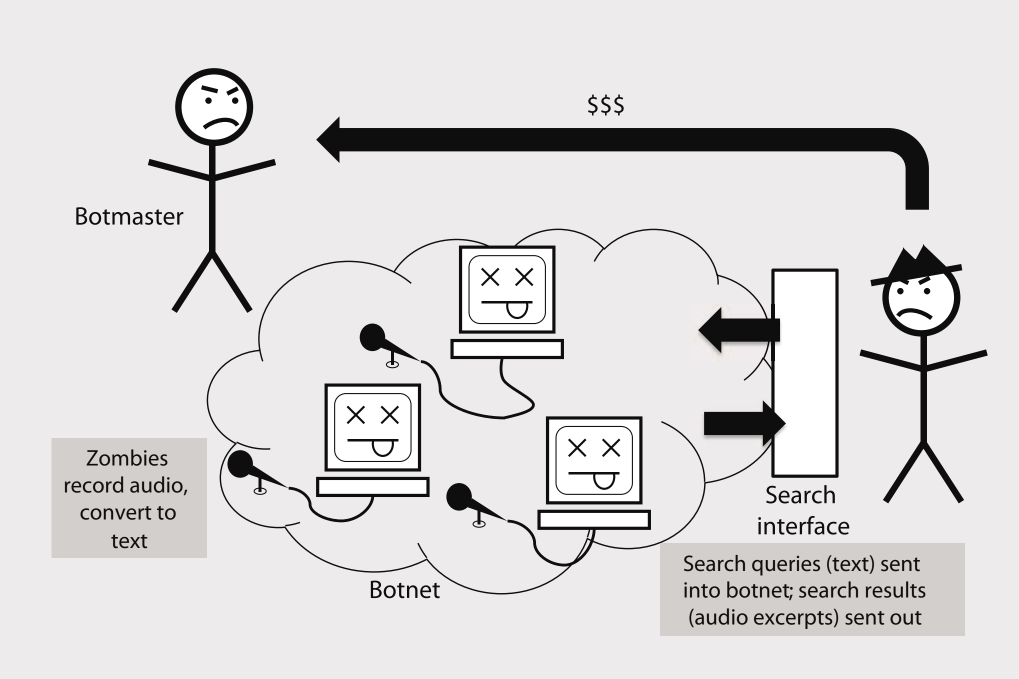
However, we don't see spyware taking advantage of this. The lack of attention to microphones by spyware can probably be attributed to one thing: money. More specifically, how can the data from a microphone be monetized on a large scale? Advertisers are leading the pack here, and there is no reason that adware couldn't learn the same tricks. For example, foreground and background audio may be analyzed for advertising keywords (via speech recognition) or for demographic information (Maislos07, Scott10, Yu07).

Making money from spyware eavesdropping is a harder problem. No one reads their credit card number aloud while shopping online, and even so, it would have to be recorded and found by someone wanting to steal the information.

Recording audio is actually not that daunting a task, in terms of storage space consumption. A mediocre-

References

- [Bell01] G. Bell. A personal data store. Communications of the ACM 44(1), 2001, pp. 86-91.
- [Friess08] N. Friess, J. Aycock, and R. Vogt. Black market botnets, MIT Spam Conference, 2008.
- [Gemmel06] J. Gemmel, G. Bell, and R. Lueder. MyLifeBits: A personal database for everything. Microsoft Technical Report MSR-TR-2006-23, 2006.
- [GuardiaCivil05] Guardia Civil. Detenido el creador de un virus informático que podía haber infectado a miles de usuarios en varios países, http://www.guardiacivil.org/prensa/notas/win_noticia.jsp?idnoticia=1657, 2005.
- [Kambas08] M. Kambas. Cyprus online voyeur gets 4 years for harassment, Reuters, 4 August 2008.
- [Leyden05] J. Leyden. Webcam Trojan perv gets slapped wrist. The Register, 28 February 2005.
- [Maislos07] A. Maislos, R. Maislos, and E. Arbel. Method and apparatus for electronically providing advertisements. United States Patent Application 20070186165, 2007.
- [OGrady08] J. O'Grady. Apple Inc., Greenwood Press, 2008.
- [Scott10] C. Scott, S. White, and A. Mukerji. Method and apparatus for analyzing discussion regarding media programs. United States Patent Application 20100228547, 2010.
- [Voyles08] K. Voyles. Computer voyeurism lands student in jail. The Gainesville Sun, 1 August 2008.


$$$
Botmaster
Zombies record audio, convert to text
Botnet
Search interface
Search queries (text) sent into botnet; search results (audio excerpts) sent out

quality audio file, by which I mean a Justin Bieber song, only weighs in around four megabytes; a recording of sporadic conversation need not be large, a gigabyte per month (Gemmel06). In fact, it's estimated that recording an entire lifetime's worth of audio is already well within our capacity (Bell01, Gemmel06).

Finding and selling interesting data, needles in virtual haystacks, is the specialty of a "black market" botnet (Friess08). A botmaster establishes a botnet and sets its zombies recording and converting the audio into text. The botmaster also builds a search interface so that *other* people can search for interesting audio recordings to purchase. The strength of this model is that the botmaster doesn't need to know what audio recordings are valuable. The botmaster simply acts to facilitate malicious acts by other people.

Alternatively, the botmaster can send short audio excerpts from zombie machines to Mechanical Turks, perhaps low-paid people in developing countries, to listen for interesting audio worth retrieving and exploiting. Humans, not computers, do the pattern matching: not every technical problem requires a technical solution.

And thus the Ear of Sauron begins to listen.

John's new book Spyware and Adware *is available from Springer.*

JOHN AYCOCK
Department of Computer Science
University of Calgary, Canada
aycock@ucalgary.ca