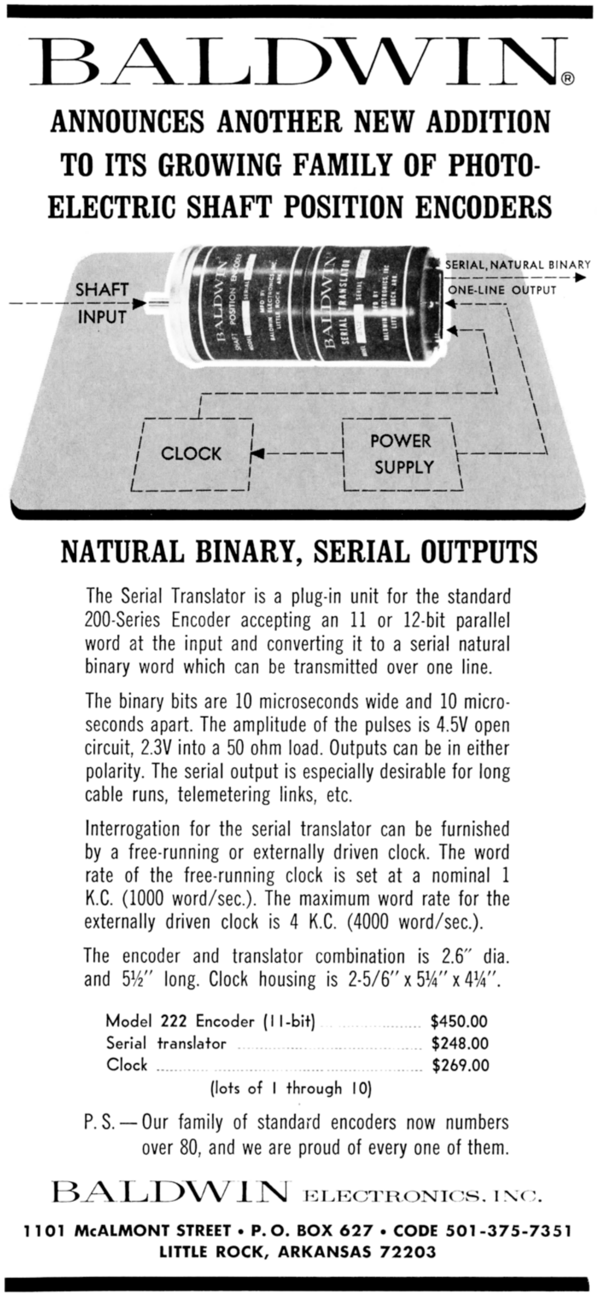
22:01 Need something good to read, my good neighbor?

Neighbors, please join me in reading this twenty-third release of the International Journal of Proof of Concept or Get the Fuck Out, a friendly little collection of articles for ladies and gentlemen of distinguished ability and taste in the field of reverse engineering and the study of weird machines. This release is a gift to our fine friends in Washington, D.C.



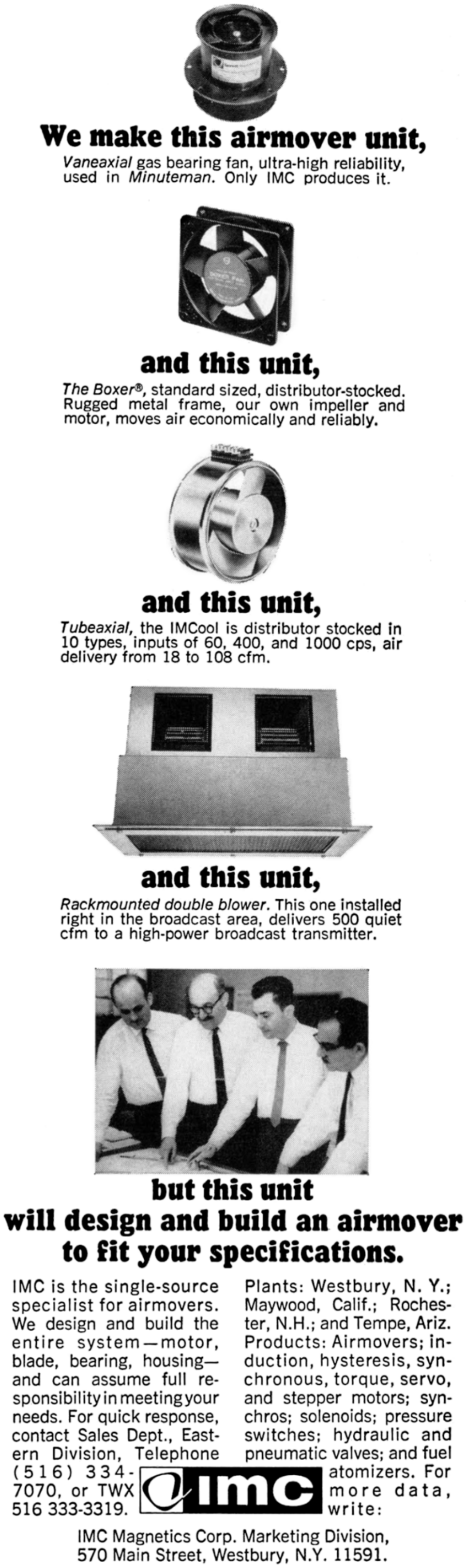
If you are missing the first twenty two releases, we suggest asking a neighbor who picked up a copy of the first in Vegas, the second in São Paulo, the third in Hamburg, the fourth in Heidelberg, the fifth in Montréal, the sixth in Las Vegas, the seventh from his parents' inkjet printer during the Thanksgiving holiday, the eighth in Heidelberg, the ninth in Montréal, the tenth in Novi Sad or Stockholm, the eleventh in Washington D.C., the twelfth in Heidelberg, the thirteenth in Montréal, the fourteenth in São Paulo, San Diego, or Budapest, the fifteenth in Canberra, Heidelberg, or Miami, the sixteenth release in Montréal, New York, or Las Vegas, the seventeenth release in São Paulo or Budapest, the eighteenth release in Leipzig or Washington, D.C., the nineteenth in Montréal, the twentieth in Heidelberg, Knoxville, Canberra, Baltimore, or Raleigh, the twenty-first in Leipzig or Washington, D.C., or the twenty-second in D.C. Three collected volumes are available from No Starch Press, wherever fine books are sold.

On page 5, Travis Goodspeed shares his tools for reverse engineering a photograph of a mask ROM into a ASCII art bitstream, and then converting that physically ordered bitstream into logically ordered bytes that might work in a disassembler or emulator. If you need to reverse engineer microcontroller firmware from before flash memory became cheap and plentiful, this is the tool for you.

Ange Albertini wrote PoC||GTFO 7:6, the classic article on abusing file formats with polyglots. On page 11, he presents a follow-up with better classifications and the idea of "polymocks," which are not polyglots but easily confuse `libmagic` and its friends into believing that file is valid in dozens of formats.

Eighty years ago, C.S. Lewis published the Screwtape Letters, a classic of apologetics presented as letters from a senior demon named Screwtape to his junior nephew, Wormwood. On page 17, Pastor Laphroaig shares with us a more recent set of mis-delivered letters, in which Wormwood—now a senior demon—writes to his young nephew Malört about modern video clips, computer programming and how hard it is for a concerned demon to earn the wages of sin.

On page 19, Ange presents a series of tricks building up to generic, reusable hash collisions for tarballs and zipped XML files, such as `.docx` files.



Windows, LLVM and Grsecurity all have control flow integrity schemes that can restrict the targets of indirect calls, such as function pointers. Aleksandar Nikolic has been playing with the eXtended Flow Guard scheme from Windows 11, using the hashed integrity markers as a means of reverse engineering the calling conventions of functions. What began as a mitigation against memory corruption exploits has become an oracle for reverse engineering!

Stefan Kölbl and Ange Albertini have been playing around with CTR mode, coming up with near-polyglots that have a different meaning and file format for each of a few different key/nonce pairs. Page 30.

A long time ago in an evil empire far away, the Soviet Union's consumer electronics monopoly produced a pocket calculator, the Электроника MK-51. This looks exactly like Casio's fx-2500, and on page 32, Travis Goodspeed deconstructs both calculators to show that the MK-51 counterfeits not just the look and feel of the Casio, but also its NEC microcontroller and every last bit of mask ROM.

We've recently been including tourist guides to new computer architectures, and this release is no exception. Christopher Hewitt and Niccolò Izzo describe the M16C and R8C series of microcontrollers from Renesas on page 39, beginning with the basics and working their way up to a fault injection attack. EVM can't let them have all the fun, so page 46 presents his guide to the Elbrus 2000 architecture, Russia's domestically designed VLIW architecture with register windowing.

Harvey Phillips shares on page 52 his Janus polyglot from the Binary Golf Grand Prix. It's valid as an x86 bootloader, ELF, COM, RAR, and a GNU Multiboot2 image, but also as program for the Commodore 64! To keep the size to a minimum, many of these formats have useful sections overlapping.

On page 68, we pass the collection plate, not for bitcoins or wooden nickels, but for nifty stories. What fine stories do you have, left untold except at your local pub? With what clever tricks might you grace our readers?