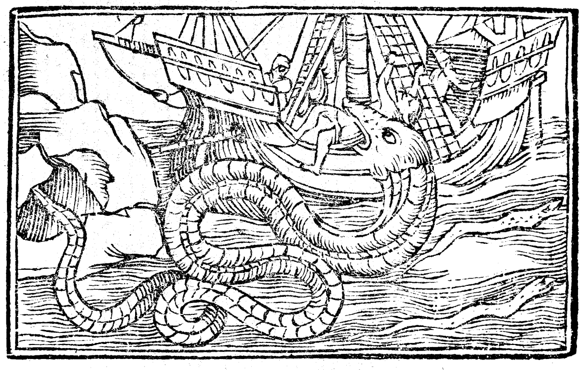
1 Please stand; now, please be seated.

Neighbors, please join me in reading this twelfth 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 software exploitation and the worship of weird machines. This is our twelfth release, given on paper to the fine neighbors of Heidelberg.

If you are missing the first eleven issues, we the editors suggest pirating them from the usual locations, or on paper from 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, or the eleventh in Washington, D.C.

Our own Pastor Laphroaig opens this issue on page 4 by confessing to be a fan of junk hacking! He tells us to ignore the publicity and drama around a hack, to ignore even its target and its CVE. Instead, we should learn the mechanism of the hack, the clever tricks that make it work. Programming these mechanisms in nifty ways, be they ever so old, is surely not "junk"—think of it instead as an educational journey to far and exotic shores, on which this issue's great crew of authors stands ready to take you, neighbors!

In a fit of nostalgia for the good old vector arcade games, Trammel Hudson extended MAME to support native vector displays of the 1983 Star Wars arcade game on both his Tektronix 1720 scope and a Vectrex home vector display. Find it on page 6.



Eric Davisson contributes a 512-byte game for the PC BIOS on page 9. He discusses some nifty tricks for self-rewriting code in 16-bit Real Mode and shows that the fancier features of an operating system aren't needed to have a little fun—and that programming a constrained environment can be great fun indeed!

On page 15, Peter Ferrie describes his work toward a universal bypass for the `E7` protection mode used on a number of Apple][disks. This is a follow up to his encyclopedic coverage of protection modes for this platform in PoC||GTFO 10:7.

Ryan Speers and Travis Goodspeed have begun a series of tourist guides, intended to quickly introduce reverse engineers to a new platform. Page 20 provides a lightning-fast introduction to ARM's Cortex M series, which you'll find in modern devices with a megabyte or less of Flash memory. Page 28 contains similar notes for the Texas Instruments MSP430, MSP430X, and MSP430X2 architectures, a 16-bit competitor to the PIC and AVR.

At this journal, we generally frown upon defense, not because it is easy, but because it is so damned hard to describe properly. On page 24, Jeffrey Crowell presents a poor man's method of patching 32-bit x86 binaries to enforce the control flow graph. With examples in Radare2 and legible C, you'll be itching to write your own generic patchers for large binaries this weekend.

Page 33 describes how Evan Sultanik made this PDF—the one that you're reading—into a poyglot webserver quine in Ruby with its own самиздат PoC||GTFO mirror.

It is with great sadness that we dedicate this release to the memory of our neighbor Ben Byer, the "hypothetical defendant by the name of 'Bushing'" who inspired many of us to put pwnage before politics, to keep on hacking. We're gonna miss him.

– – – –   – – –   – – – –

On page 40, the last page, we pass around the collection plate. We're not interested in your dimes, but we'd love some nifty proofs of concept. And remember, one hacker's "junk hacking" may hold the nifty tricks needed for another's treasured exploit!