1 Lisez Moi!

Neighbors, please join me in reading this thirteenth 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 release is given on paper to the fine neighbors of Montréal.

If you are missing the first twelve 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, the eleventh in Washington, D.C., or the twelfth in Heidelberg.

We begin on page 4 with a sermon concerning peak computation, population bombs, and the joy of peeks and pokes in the modern world by our own Pastor Manul Laphroaig.

On page 6 we have a *Z-Wave Christmas Carol* by Chris Badenhop and Ben Ramsey. They present a number of tricks for extracting pre-shared keys from wireless Z-Wave devices, and then show how to use those keys to join the network.

On page 14, Krzysztof Kotowicz and Gábor Molnár present *Comma Chameleon*, weaponize PDF polyglots to exfiltrate data via XSS-like vulnerabilities. You will never look at a PDF with the same eyes again, neighbors!

Chris Domas, whom you'll remember from his brilliant compiler tricks, has contributed two articles to this fine release. On page 28, he explains how to implement *M/o/Vfuscator as a Virtual Machine*, producing a few bytes of portable C or assembly and a complete, obfuscated program in the `.data` segment.

IBM had JCL with syntax worse than Joss, and everywhere the language went, it was a total loss! So dust off your z/OS mainframe and find that ASCII/EBCDIC chart to read Soldier of Fortran's *JCL Adventure with Network Job Entries* on page 32.

What does a cult Brezhnev-era movie have to do with how exploit code finds its bearings in a Windows process' address space? Read *Exploiting Weak Shellcode Hashes to Thwart Module Discovery; or, Go Home, Malware, You're Drunk!* by Mike Myers and Evan Sultanik on page 57 to find out!

Page 63 begins Alex Ionescu's article on a *DeviceGuard Mitigation Bypass for Windows 10*, escalating from Ring 3 to Ring 0 with complete reconstruction of all corrupted data structures.

Page 72 is Chris Domas' second article of this release. He presents a Turing-complete *Virtual Machine for VIM* using only the normal commands, such as yank, put, delete, and search.

On page 76 you will find a rousing guest sermon *Doing Right by Neighbor O'Hara* by Andreas Bogk, against the heresy of "sanitizing" input as a miracle cure against injection attacks. Our guest preacher exposes it as fundamentally unneighborly, and vouchsafes the true faith.

Concluding this issue's amazing lineup is *Are androids polyglots?* by Philippe Teuwen on page 79, in which you get to practice Jedi polyglot mind tricks on the Android package system. Now these *are* the droids we are looking for, neighbors!

– — — – — — — – — – –

On page 80, 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!