Children's Bible Coloring Book of PoC || GTFO
Issue 0x02, an Epistle to the 30th CCC Congress in Hamburg

Composed by the Rt. Revd. Pastor Manul Laphroaig to put pwnage before politics.
pastor@phrack.org

December 28, 2013

1 Call to Worship

Please join me in reading this third issue 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. If you are missing the first two 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 or the second in São Paulo.

This edition is written to the fine neighbors of the Chaos Computer Club in honor of their thirtieth congress, to be held this December in Hamburg. As in prior issues, you'll find plenty of pwnage, some neighborly preaching, and no politics.

In Section 2, Pastor Laphroaig preaches that in the tradition of Noah and of Howard Hughes, we should build our own fucking birdfeeders.

Brother Myron Aub takes a break from his evangelical promotion of Graphitics to teach us a little about the PGP Message format in Section 3. It turns out that RFC 4880 gives him just enough room to encode an LZ-compression quine within a message, and the PGP interpreter is just "smart"[1] enough to keep decoding it 'till the cows come home. Perhaps other weird machines remain to be found?

Natalie Silvanovich shares in Section 4 her techniques for reliably dropping shellcode into the Tamagotchi's 6502 controller from malicious plugin cartridges. Her exploit requires a number of nifty tricks, not least of which is that the some bits of the program counter are ignored in this architecture, so her victim executes the right code from the wrong address! It is feared that this technology might be used

[1] Because things marketed as "smart" usually aren't, at least not for the buyer's benefit. Truly, the world does occasionally need reminding that stupid is as stupid does.

by the Royal Canadian Mounted Police to fuel a Cyber War of 1812 against the State of New Hampshire and the People's Republic of Vermont. Both American and Canadian neighbors can rest assured that this one would have the same winner as the original, Non-Cyber War of 1812.

Travis Goodspeed shares a grab-bag of tricks for exploiting microcontrollers in Section 5. Learn how to combine a Write and a Checksum primitive with weirder properties of Flash memory into a bitwise Read primitive when exploiting microcontrollers, how to NOP-out instructions without erasing Flash pages, and how to use bootloader ROMs for a return-to-libc attack.

Bx Shapiro had a nifty article in PoC||GTFO 0:5 in which she showed out to return from ELF to libc. That article ended with a challenge to our readers, asking you fine folks to figure out how in living hell parameters could be passed to the function beging called. In Section 6, she rises to her own challenge, showing you how to call putchar() from an ELF Weird Machine without having any of your own native code.

Dave Weinstein in Section 7 explains why `POKE 62975, 0` will brick a Trash 80 Model 100 until that poor machine is put out its misery by a cold reset. Feel free to try it out in your emulator and consider that many Automatic Exploit Generators aren't very good at predicting the effects of a write-once-anywhere vuln.

Ange Albertini explains the internal organization of this issue's PDF in Section 8. Curious readers might want to run `qemu-system-i386 -fda pocorgtfo02.pdf` in order to experience all the neighborliness that this issue has to offer.

In PoC||GTFO 01:02, Dan Kaminsky shared with us a 4-line RNG for Javascript, challenging our readers to exploit it. It had no whitening, no scrambling, and no other defenses, so any weakness in the principle ought to have been exploitable. In proper PoC||GTFO fashion, Joernchen demonstrates such a vulnerability in Section 9, by observing that some versions of Firefox bias toward producing bytes of low Hamming weight.

Section 10 contains Ben Nagy's latest masterpiece, sure to get you, dear reader, on all sorts of watchlists. We half-heartedly apologize in advance to any of our readers at spooky agencies who have to explain having this magazine to their employers.

Finally, in Section 11, we do what churches are best at and pass the collection plate. Please consider giving alms of 0day and PoC to those who are poor in spirit.

Artwork in this issue was created by Ra of Tama-Zone, Stefan Bauwens, and others. The painting featured in the museum on page 31 is in remembrance of the one first drawn by Mirromaru in red creeper cards at the 29th Congress, then quickly censored due to controversy.

— — — —

We the editors are aware that some of the illustrations might be offensive to our more sensitive readers, either for reasons of vulgarity or blasphemy. In both cases, we rely on the Bill Hicks Defense.

"Buddy, we're Christians, and we don't like what you said."

"So forgive me!"