delCEr

github.com/f0wl/delCEr

f0wl

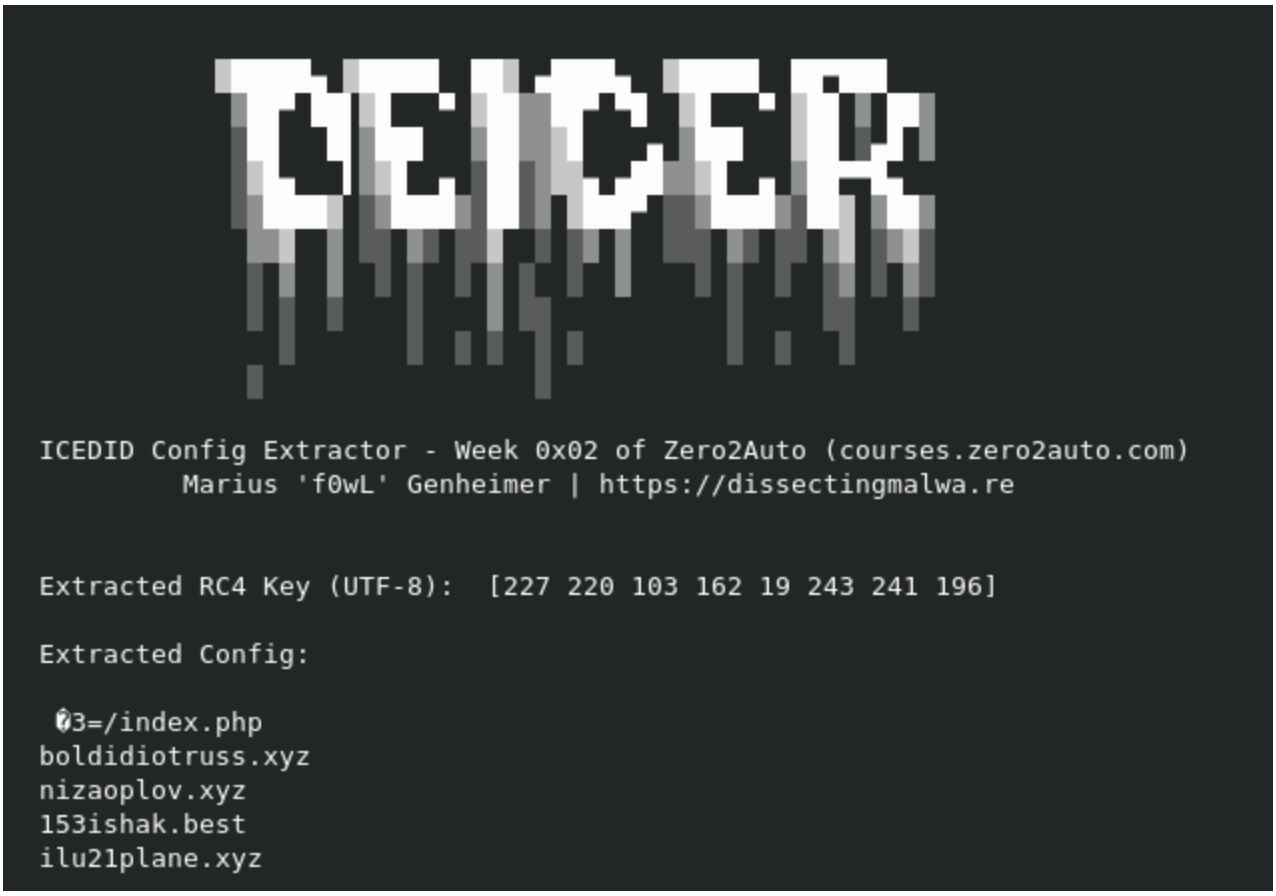
f0wl/delCEr

A crude Config Extractor for IcedID second stage Loaders (Zero2Auto Week 0x02)

1 Contributor 0 Issues 3 Stars 1 Fork

go report A+

A crude Config Extractor for IcedID second stage Loaders (Zero2Auto Week 0x02)



If you need a sample to test it with check out this one on Malshare (already unpacked for your convenience)