

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)



ICEDID Config Extractor - Week 0x02 of Zero2Auto (courses.zero2auto.com)
Marius 'f0wL' Genheimer | <https://dissectingmalwa.re>

Extracted RC4 Key (UTF-8): [227 220 103 162 19 243 241 196]

Extracted Config:

```
03=/index.php  
boldidiotruss.xyz  
nizaoplov.xyz  
153ishak.best  
ilu21plane.xyz
```

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