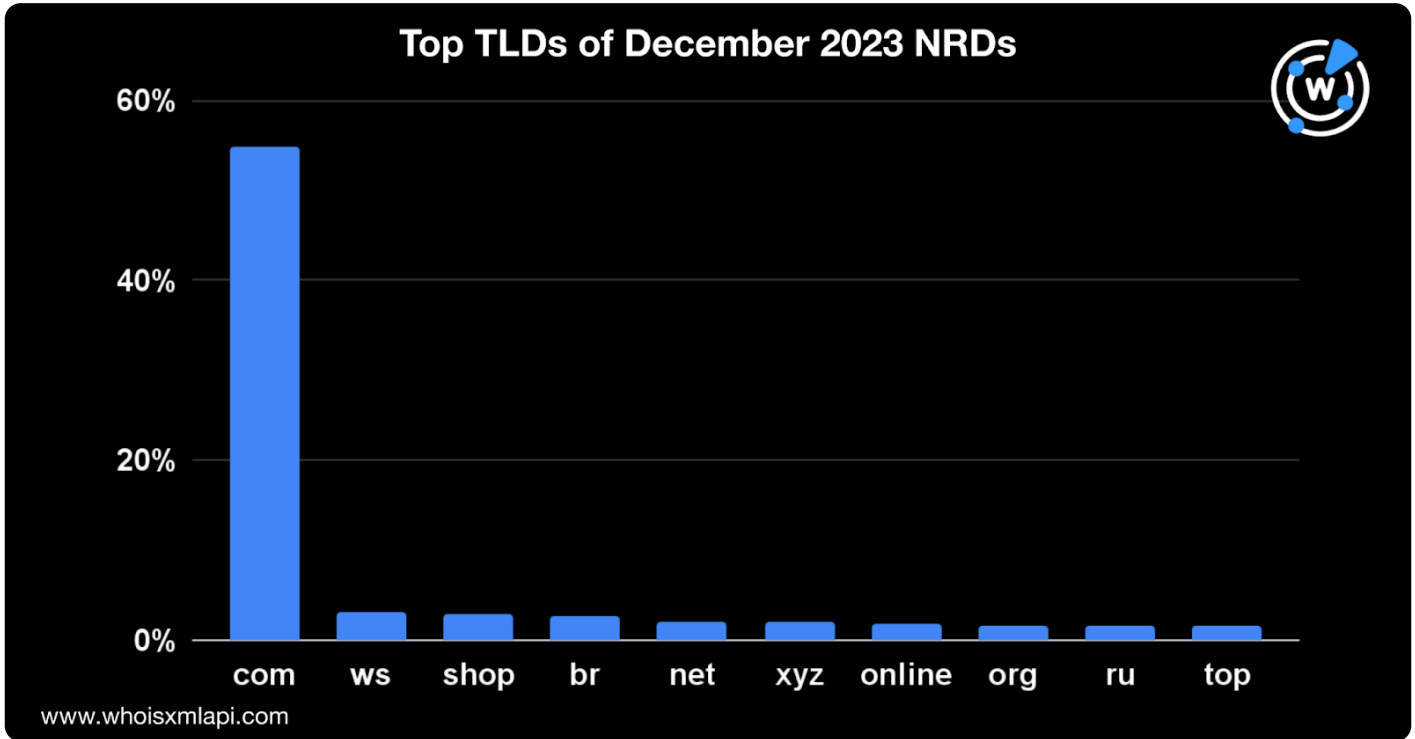
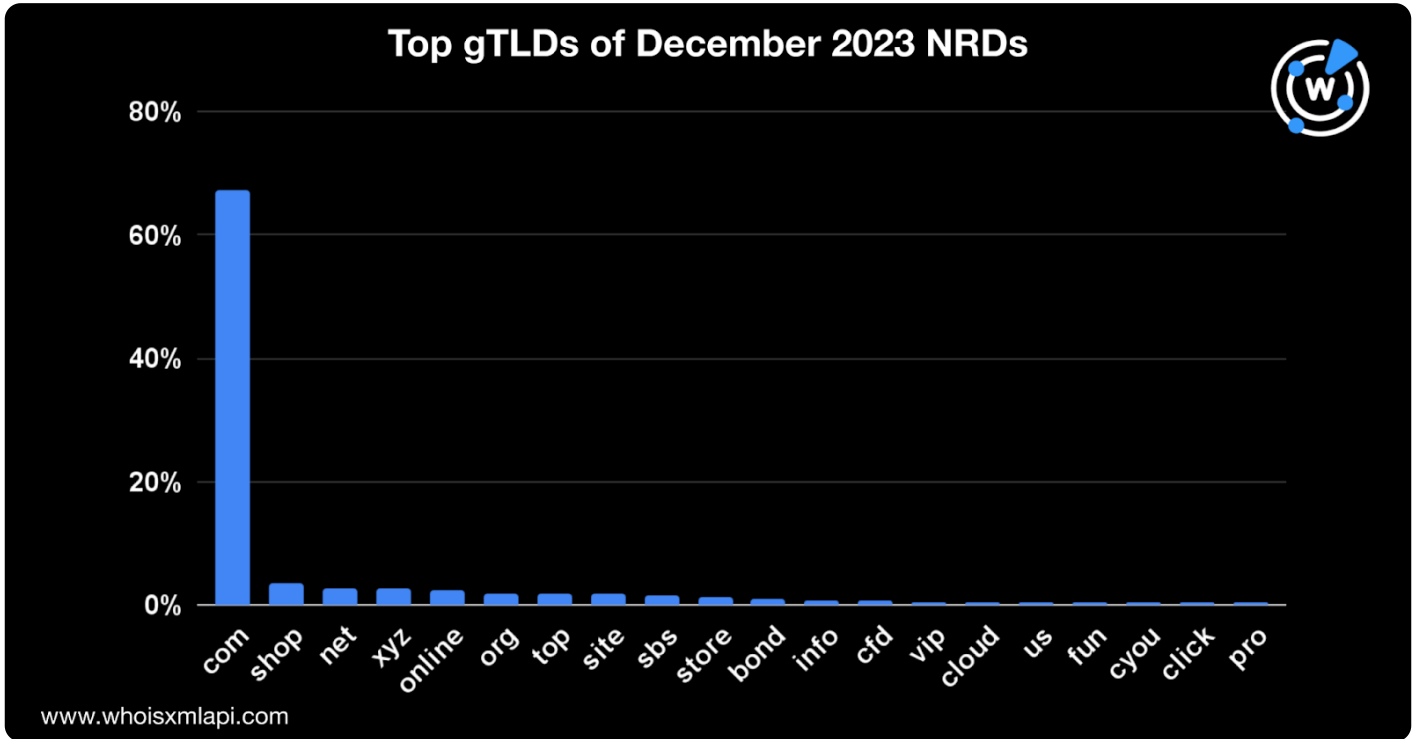


?????.com????????????????????54.8%?????????.ws????3.1%?.shop????3%?.br????2.7%?.net?.xyz??????2.1%?.org????1.6%?.ru?.top??????1.5%??

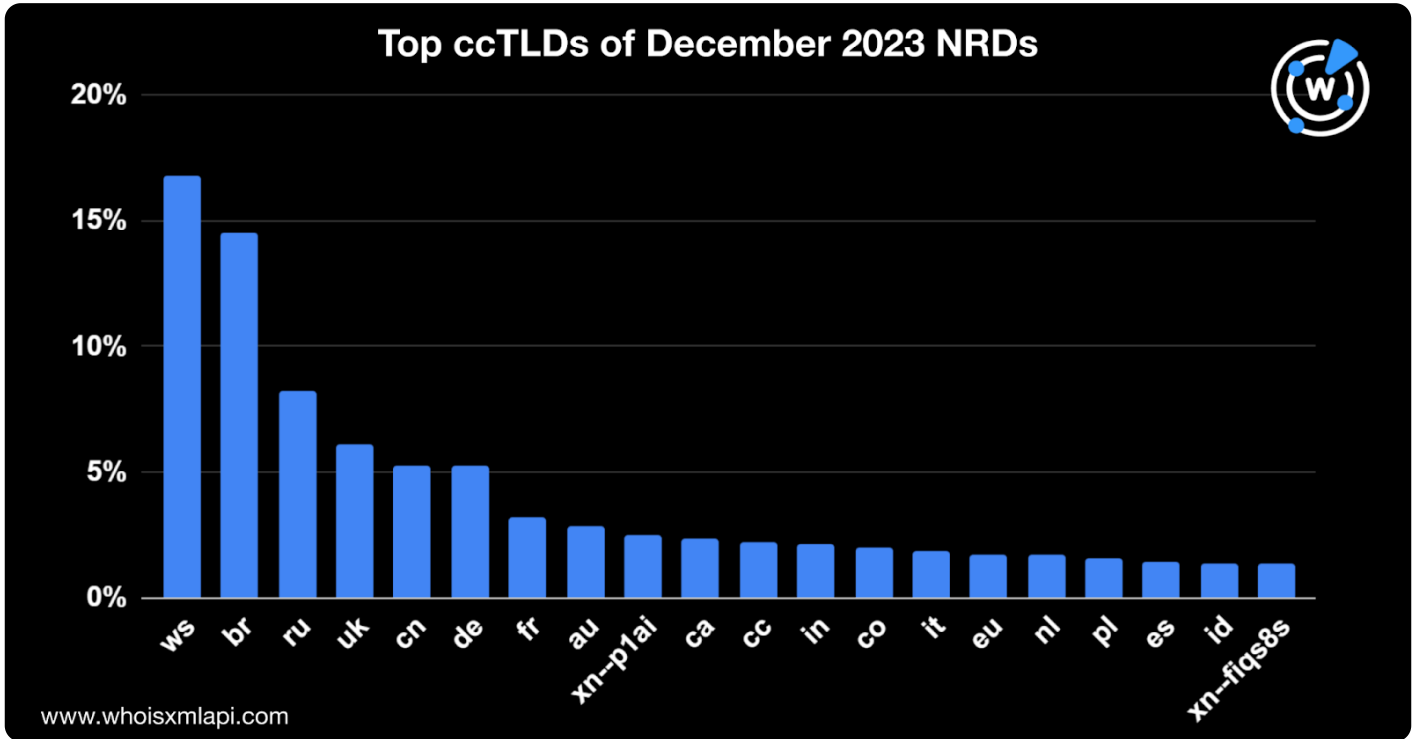


??

625?????????.com??67.3%????20?????????????.com?????????????
? .xyz(??? 2.6%)?.online(2.4%)?.org ? .top (??? 1.9%)?.site (1.8%)?.sbs (1.6%)?.store ? .bond
(??? 1.2%)?.info (0.9%)?.cfd (0.7%)?.vip?.cloud?.us ? .fun (??? 0.5%)???? .cyou?.click ? .pro (???
0.4%)?

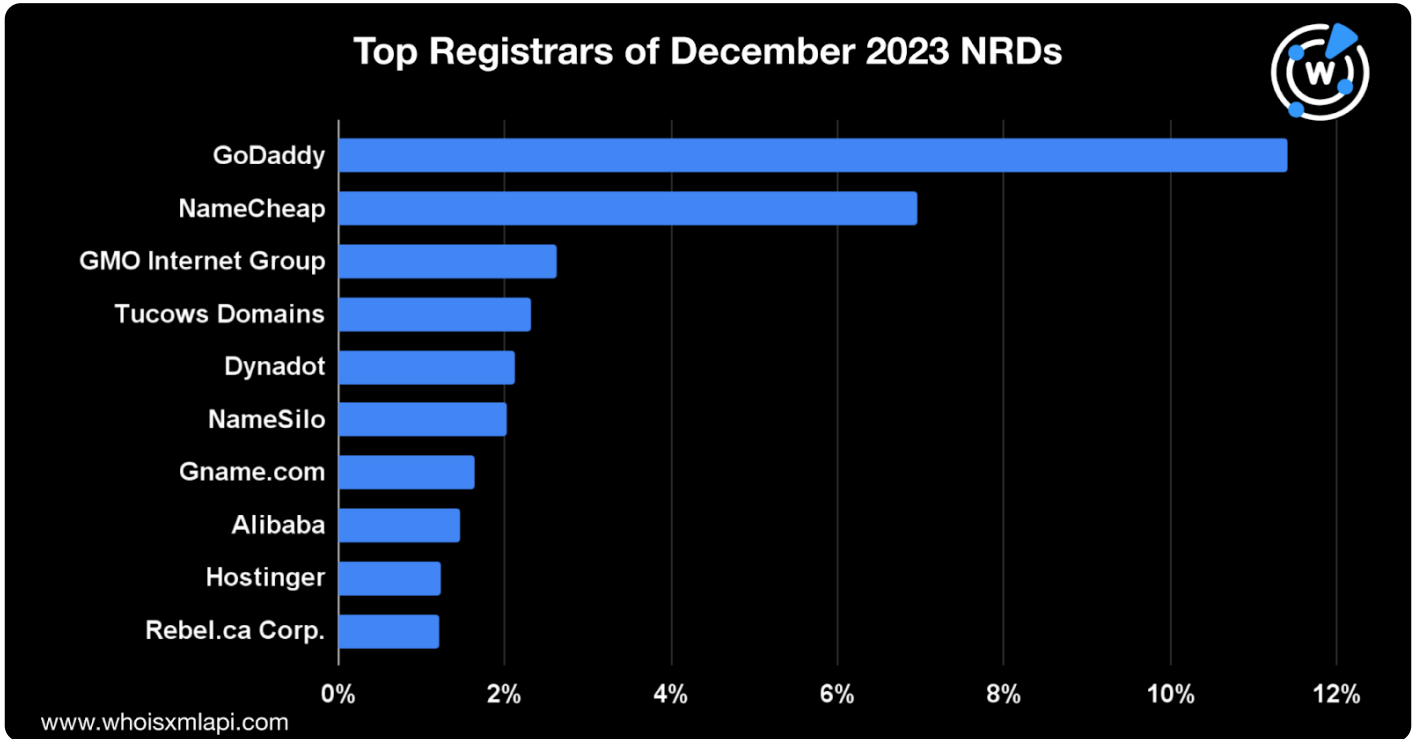


240 .ws 12 16.8% .br 14.6% .ru 8.3% .uk 6.1% .cn 5.2% .fr 3.2% .au 2.8% .xn--p1ai 2.5% .ca 2.4% .cc 2.2% 20



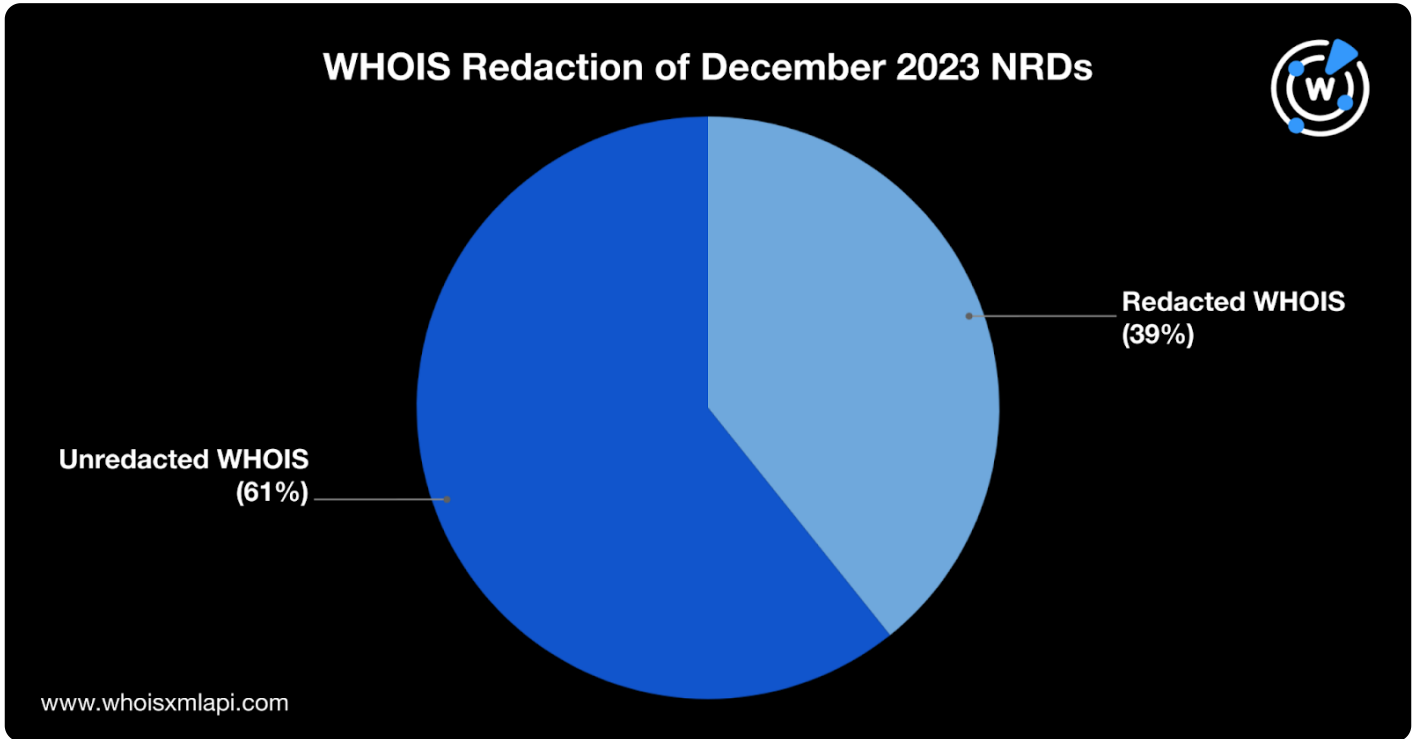
?????

GoDaddy 11.4% Namecheap 7.7% GMO Internet 2.6% Tucows 2.3% Dynadot 2.1% NameSilo 2% Gname 1.6% Hostinger 1.5% Rebel.ca 1.2%



WHOIS????

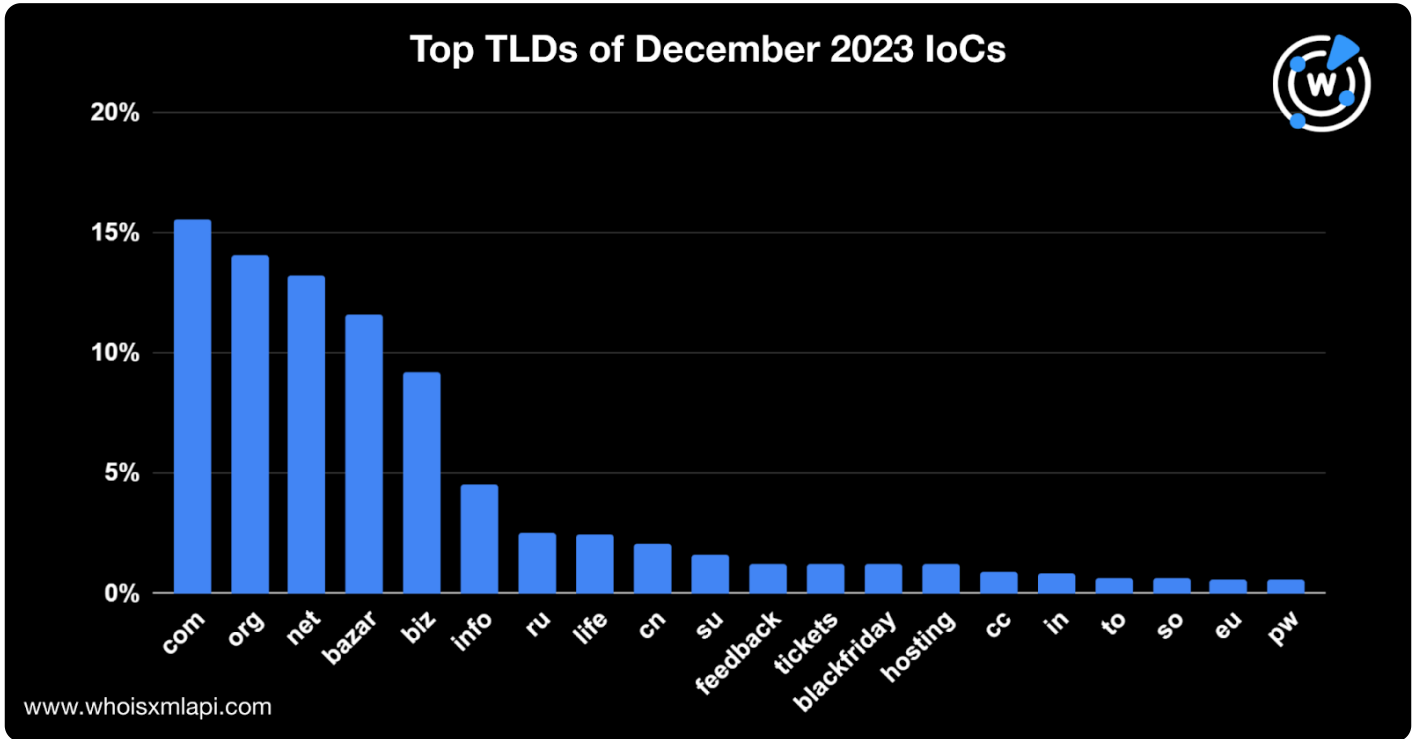
12????????????61%????????????WHOIS?????39%????????????WHOIS?????????



?DNS??????????????

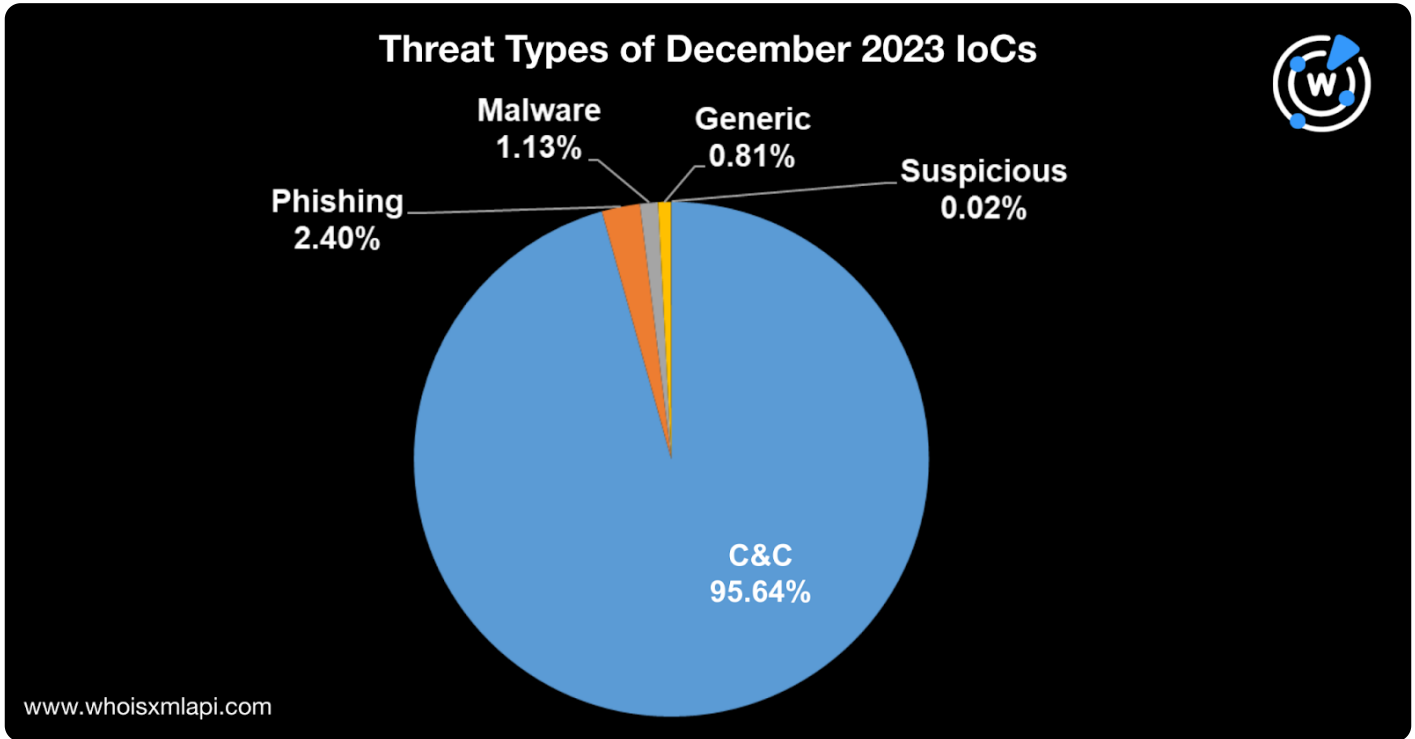
12??loCs??????????

?????12?????????150??loC?????????????????16%?????.com?????????????????loC?????????????????.org
(14%) ?.net
(13%)?????????????????12%???.bazar?9%???.biz?5%???.info?2%???.life?????????????????????.ru
(3%)?.cn ? .su (??? 2%)?????? loC ??? 20 ???????????



12??IoCs??????

??????12?????? IoC ?????????????????????? IoC ?????????? (C&C) ???????95.64%??2.4%
 ??????????1.13% ??????????? 0.8% ??????????????????0.02% ?????????????????????



????

?????12????????????????

- **??DNS????WailingCrab?????**
 ???WailingCrab????????24????????????????????????????????3,000????????????????
- **??Atomic Stealer?????“???”?WhoisXML API?????????????????Atomic Stealer?????IoCs?????????????IP????????????????????**
- **DNS ????????????????????? Dancho Danchev**
 ???
- **?????????Genesis Market?????????????DNS????????????????????????? IP ?????????? Genesis Market ??????????????????**

????????????????

??