IRC attack:

192.168.2.112 ->131.202.243.84

192.168.5.122 ->198.164.30.2

192.168.2.110 -> 192.168.5.122

192.168.4.118 -> 192.168.5.122

192.168.2.113 -> 192.168.5.122

192.168.1.103 -> 192.168.5.122

192.168.4.120 -> 192.168.5.122

192.168.2.112 -> 192.168.2.110

192.168.2.112 -> 192.168.4.120

192.168.2.112 -> 192.168.1.103

192.168.2.112 -> 192.168.2.113

192.168.2.112 -> 192.168.4.118

192.168.2.112 -> 192.168.2.109

192.168.2.112 -> 192.168.2.105

192.168.1.105 -> 192.168.5.122

Neris: 147.32.84.180

RBot: 147.32.84.170

Menti: 147.32.84.150

Sogou: 147.32.84.140

Murlo: 147.32.84.130

Virut: 147.32.84.160

IRCbot and black hole1: 10.0.2.15

Black hole 2: 192.168.106.141

Black hole 3: 192.168.106.131

TBot: 172.16.253.130, 172.16.253.131, 172.16.253.129, 172.16.253.240

Weasel: Botmaster IP: [74.78.117.238](tel:74.78.117.238), Bot IP: 158.65.110.24

Zeus(zeus sample 1 and 2 and 3, bin\_zeus): 192.168.3.35, 192.168.3.25, 192.168.3.65, 172.29.0.116

Osx\_trojan : 172.29.0.109

Zero access(zero access 1 and 2): 172.16.253.132, 192.168.248.165

Smoke bot: 10.37.130.4

List of all malicious ips:

|  |  |  |
| --- | --- | --- |
| 192.168.2.112 | 131.202.243.84 | 192.168.5.122 |
| 198.164.30.2 | 192.168.2.110 | 192.168.4.118 |
| 192.168.2.113 | 192.168.1.103 | 192.168.4.120 |
| 192.168.2.112 | 192.168.2.109 | 192.168.2.105 |
| 147.32.84.180 | 147.32.84.170 | 147.32.84.150 |
| 147.32.84.140 | 147.32.84.130 | 147.32.84.160 |
| 10.0.2.15 | 192.168.106.141 | 192.168.106.131 |
| 172.16.253.130 | 172.16.253.131 | 172.16.253.129 |
| 172.16.253.240 | [74.78.117.238](tel:74.78.117.238) | 158.65.110.24 |
| 192.168.3.35 | 192.168.3.25 | 192.168.3.65 |
| 172.29.0.116 | 172.29.0.109 | 172.16.253.132 |
| 192.168.248.165 | 10.37.130.4 |  |