| Malware Family | Number of Flows | Unique Server IPs | Number of SS Certs | Selected Ciphersuite | Certificate Subject |
|---|---|---|---|---|---|
| Bergat | 332 | 12 | 0 | TLS_RSA_WITH_3DES_EDE_CBC_SHA | www.dropbox. |
| Deshacop | 129 | 38 | 0 | TLS_RSA_WITH_3DES_EDE_CBC_SHA | *.onion |
| Dridex | 103 | 10 | 89 | TLS_RSA_WITH_AES_128_CBC_SHA | amthonoup |
| Dynamer | 372 | 155 | 3 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | www.dropbox. |
| Kazy | 1152 | 225 | 52 | TLS_RSA_WITH_3DES_EDE_CBC_SHA | *.onestore |
| Parite | 275 | 128 | 0 | TLS_RSA_WITH_3DES_EDE_CBC_SHA | *.google. |
| Razy | 564 | 118 | 16 | TLS_RSA_WITH_RC4_128_SHA | baidu. |
| Sality | 1,200 | 323 | 4 | TLS_RSA_WITH_3DES_EDE_CBC_SHA | vastusdomains. |
| Skeeyah | 218 | 90 | 0 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | www.dropbox. |
| Symmi | 2,618 | 700 | 22 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | *.criteo. |
| Tescrypt | 205 | 26 | 0 | TLS_RSA_WITH_3DES_EDE_CBC_SHA | *.onion |
| Toga | 404 | 138 | 8 | TLS_RSA_WITH_3DES_EDE_CBC_SHA | www.dropbox. |
| Upatre | 891 | 37 | 155 | TLS_RSA_WITH_RC4_128_MD5 | *.b7websites. |
| Virlock | 12,847 | 1 | 0 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 | block |
| Virtob | 511 | 120 | 0 | TLS_RSA_WITH_3DES_EDE_CBC_SHA | *.g.doubleclick. |
| Yakes | 337 | 51 | 0 | TLS_RSA_WITH_RC4_128_SHA | baidu. |
| Zbot | 2,902 | 269 | 507 | TLS_RSA_WITH_RC4_128_MD5 | tridayacipta. |
| Zusy | 733 | 145 | 14 | TLS_RSA_WITH_3DES_EDE_CBC_SHA | *.criteo. |