Chinesischer Wetterballon über dem Hackintosh-Forum?

Beitrag von „griven“ vom 8. Februar 2023, 07:33

ozw00d genau das tun wir schon 

Die Firewall prüft jedes Paket gegen diverse RBL's (Spamhaus, StopForumSpam etc.) und ist normalerweise auch recht effektiv dabei nur handelt es sich bei der Welle offenbar um noch relativ neue und unbekannte Netzwerke. Die IP's sind bunt gestreut es lässt sich also nicht mit Sicherheit sagen wo die her kommen. Aktuell haben wird unter anderem Singapur,Deutschland,Taiwan als Herkunftsländer ausgemacht denke aber das werden noch mehr werden. Den Block aus Singapur habe ich eben manuell in die Firewall gepackt. Generell mag ich es gerne vermeiden ganze Länder (Geo Location) zu banen denn damit sperrt man auch legitime User aus und das kann ja nicht das Ziel sein. Mich würde es nicht wundern wenn das alles kompromittierte Maschinen aus dem ESXi Hack sind die da gerade aktiv sind (erklärt auch ein wenig die bunte Streuung der IP's)...