Chinesischer Wetterballon über dem Hackintosh-Forum?

Beitrag von „griven“ vom 9. Februar 2023, 07:13

So schaut das aus EmilDeumel zumindest so lange bis die IP Ranges bekannt sind von denen die Angriffe aus erfolgen und in die entsprechenden Blocklisten aufgenommen sind. Was es schwer macht ist die Tatsache das die Accounts ziemlich bunt durch den Garten von Netzwerken überall auf der Welt verteilt erzeugt werden. Der Kollege heute kam mit einer IP rein die in die USA auflöst (Kalifornien) was meine Theorie eines Zusammenhangs mit dem ESXi Hack eher bekräftigt als entkräftet. Obendrein sind die auch "schlau" genug sich nicht wie üblicherweise zu verhalten es werden also nicht wie sonst gleich 4 oder 5 Accounts erzeugt und dann losgelegt sondern es ist pro IP immer nur ein Account manchmal zwei was zeigt das sie ebenfalls gelernt haben auf Automatismen wie die Erkennung von Doppelaccounts zu reagieren...