Black Basta - Internal Chat Leak - Initial Observations

Organigram and external service providers

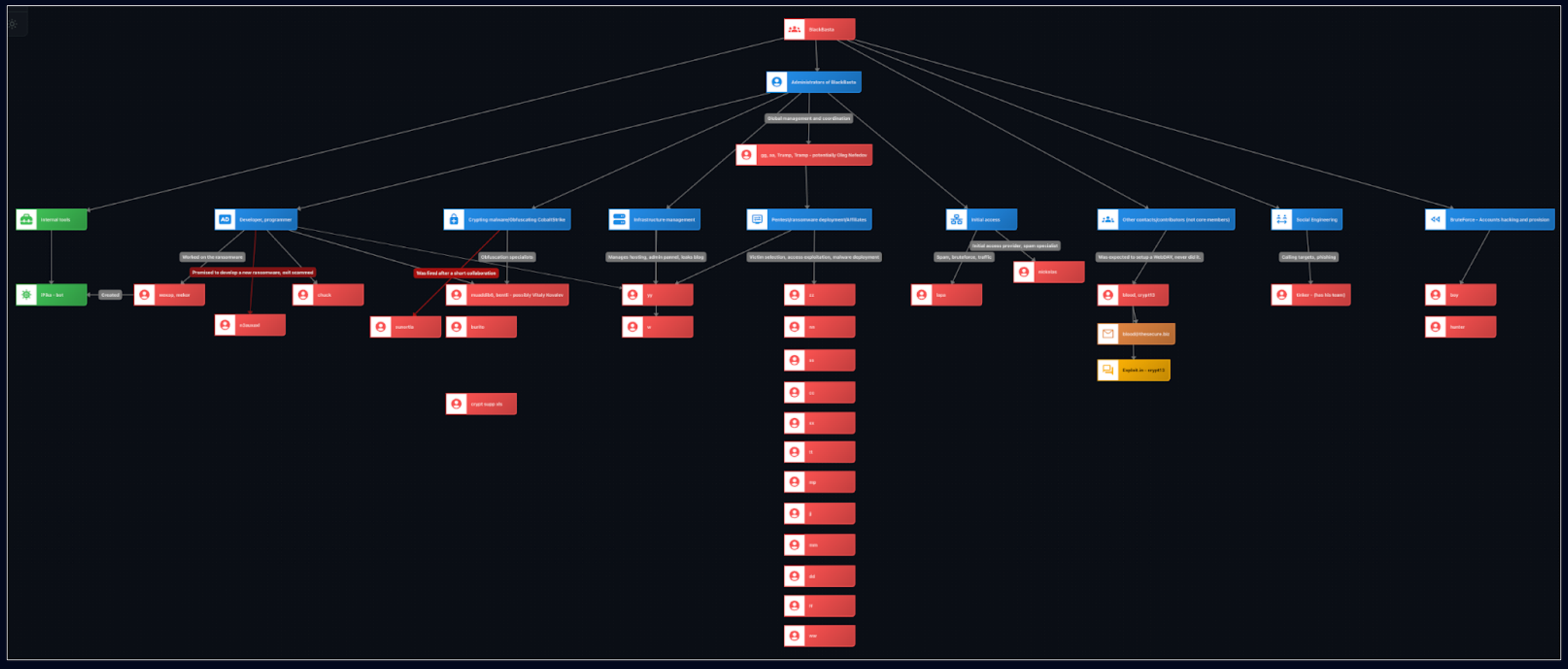

Figure 1. Organigram of Black Basta group (work in progress, stay tuned for more). Source: Flare.io

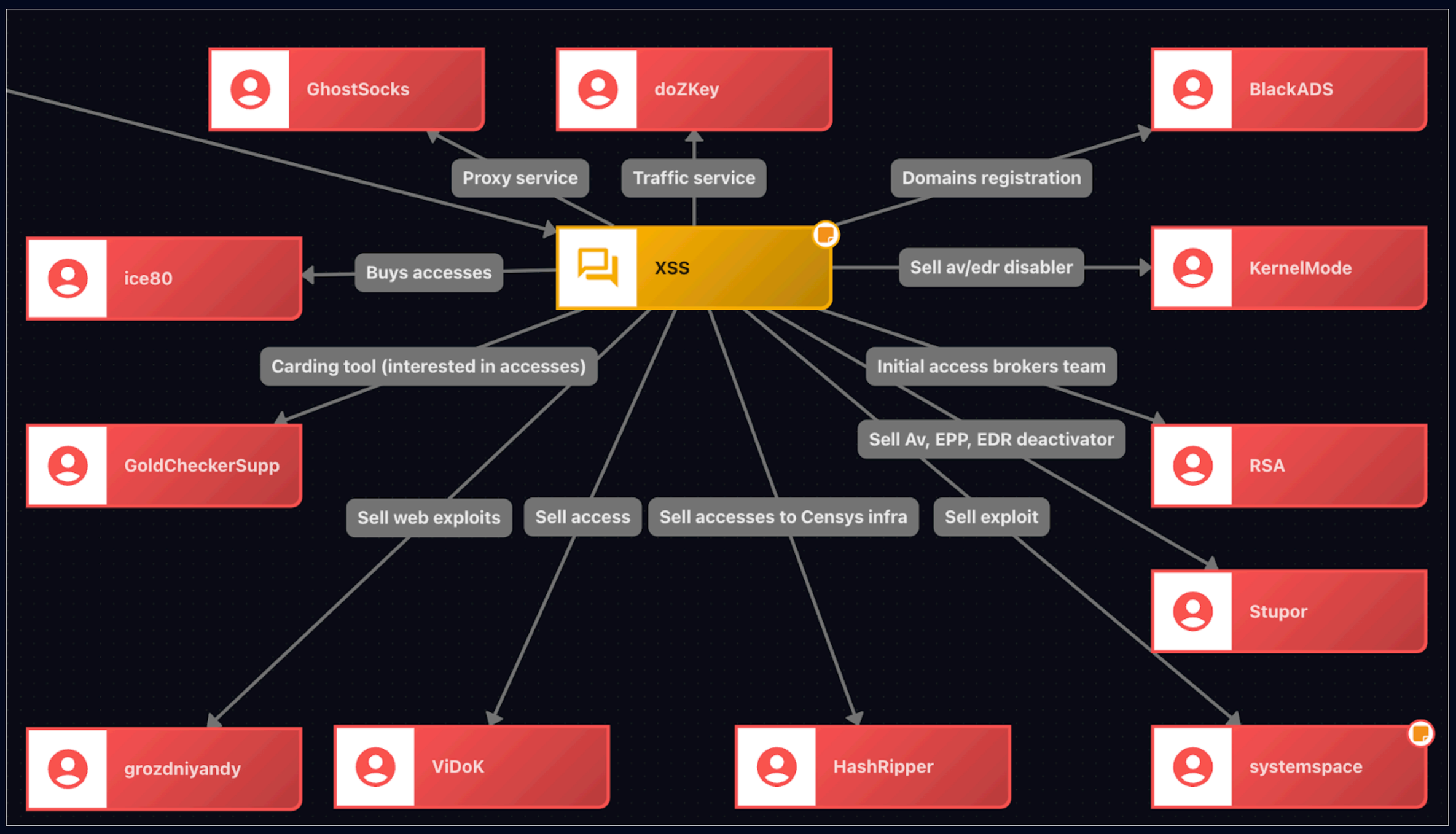

Figure 2. Potential external service providers identified in the data leak. Source: Flare.io

Black Basta Members by Number of Messages

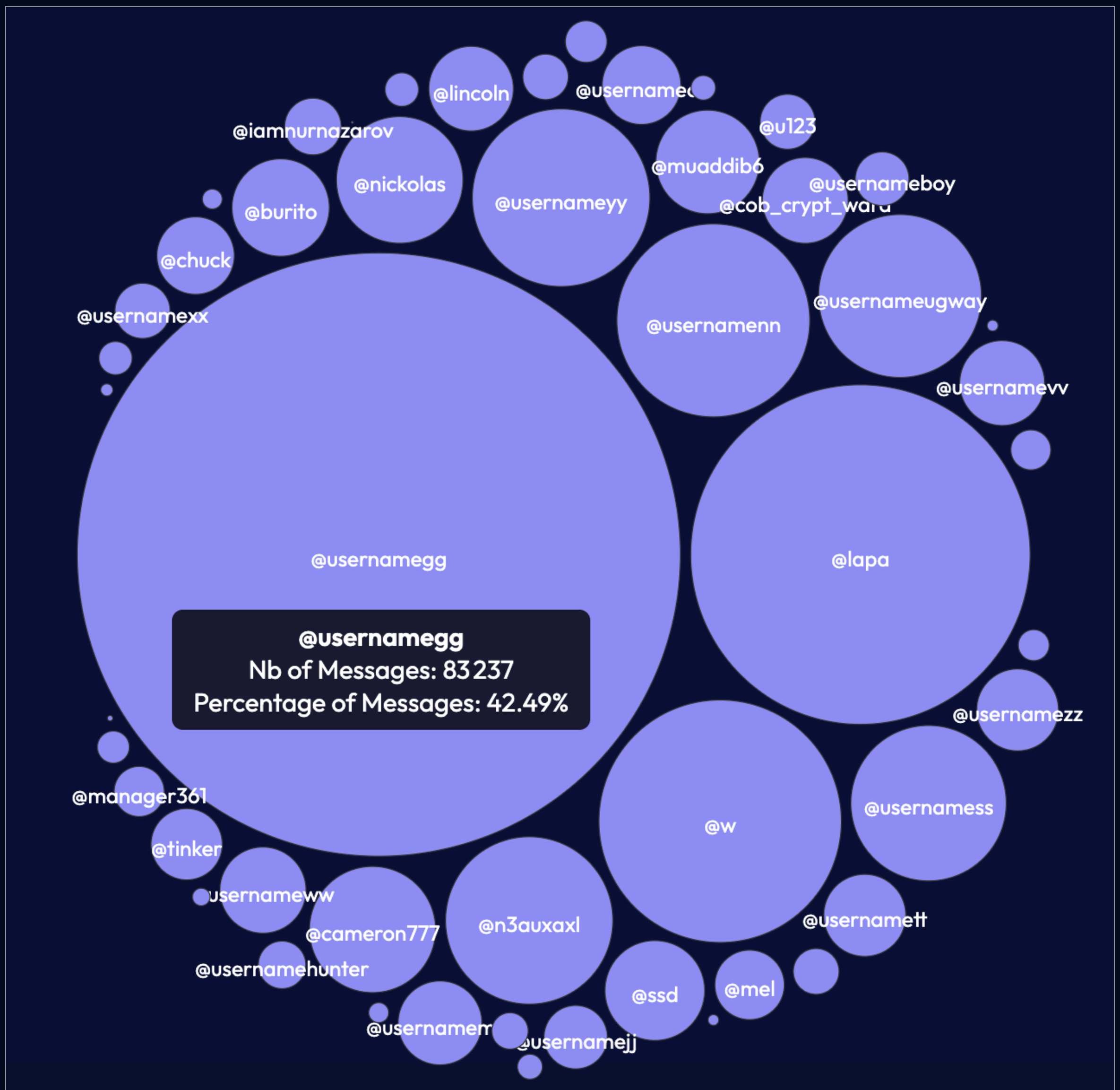

Figure 3. Chat members activity. Source: Flare.io

Among the 50 identified aliases in the leaked chat, the vast majority of messages were published by the group's leader, "gg" aka "Trump," aka "Tramp", from Conti Team 3 and members like "lapa," "w," "nn," "yy," or "n3auxaxl".

Black Basta Number of Messages by Week

Figure 4. Activity per week. Source: Flare.io

The group's activity is heavily influenced by vacation periods in Russia in January and during summer. The Orthodox New Year falls in the middle of January. Another explanation for the collapse of the messages after June is incomplete data.

Black Basta Number of Messages by Week

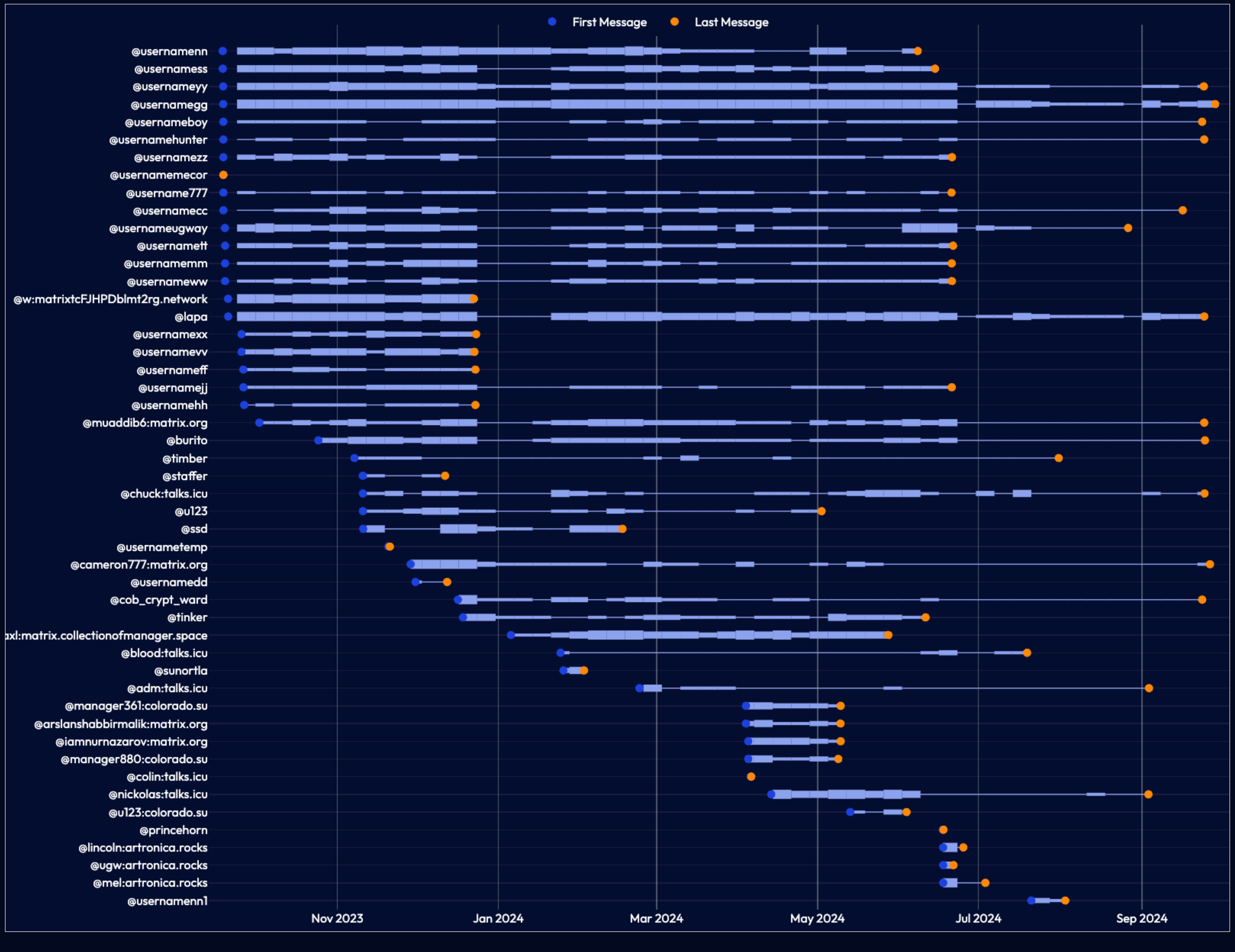

Figure 5. Detailed activity of Black Basta's members. Source: Flare.io

The theory that the dataset is incomplete is supported by the abrupt cessation of communication from several members around the end of June 2024. Our analysis of the discussions revealed no apparent reason for this sudden silence from members such as "ZZ," "tt," "JJ," and others.

flare

Black Basta’s Members Hours of Activity

Figure 6. Aggregated hours of activity of all Black Basta’s members. Source: Flare.io

The activity hours of all Black Basta members suggest that the group mainly works during office hours, like a normal business. Activity outside office hours exists but is rather rare and authored by the group’s leader and other somewhat independent members.

Black Basta’s Mentioned Vulnerabilities Types

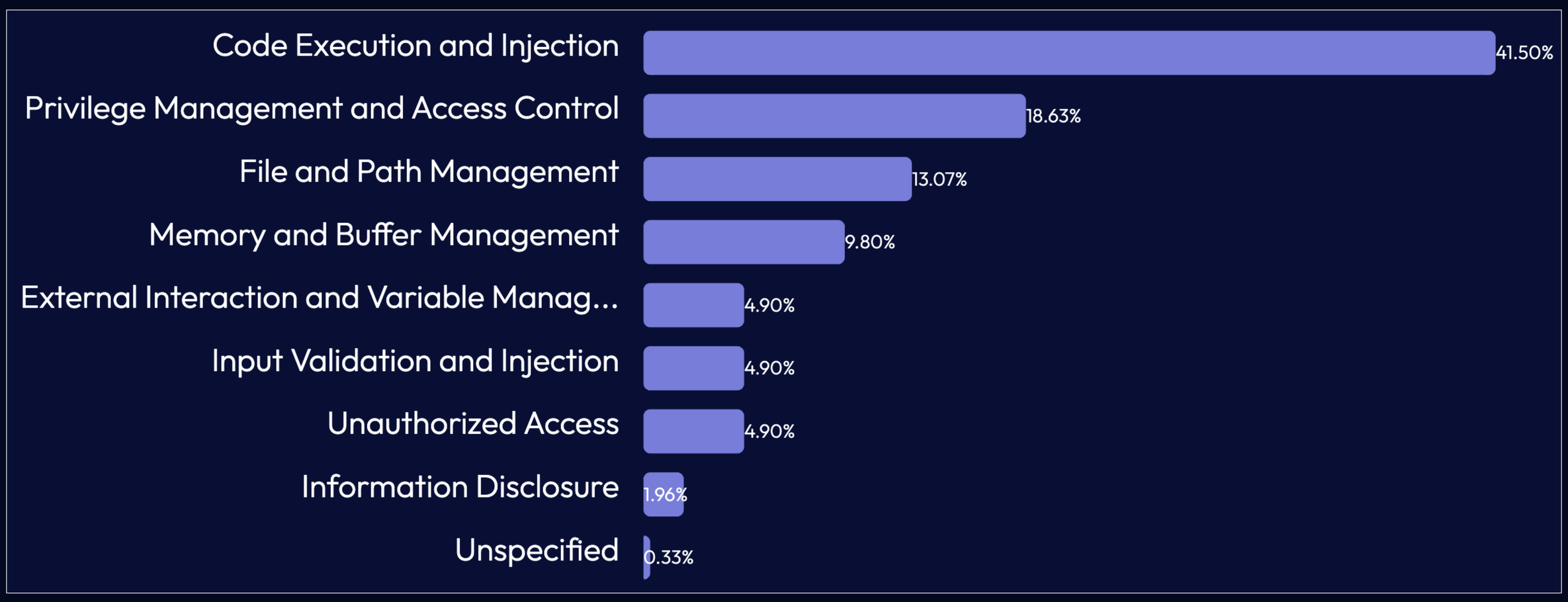

Figure 7. Percentage of mentioned vulnerabilities. Source: Flare.io

Back Basta is constantly on the hunt for new vulnerabilities and exploits. Most of the mentioned vulnerabilities affect Microsoft products (Windows, Exchange servers), Palo Alto Networks, Zimbra and Fortinet.