There are currently multiple active groups that are loosely affiliated but much information about them is not known. As a tipper, and not as a finished intelligence report, the below information is being provided on these groups.

**Dragite Group**

The Dragite Group is a series of intrusions into organizations leveraging the custom Dragite malware. This malware is unique to the group and has been observed targeting research and development organizations as well as being leveraged in the first stages of access to support ransomware and defacement campaigns. Dragite serves as a platform enabling both access operations as well as a full suite of capabilities once deployed and contains modules to support various types of operations. The name comes from the “Dragite” name being seen as a user in the PDB strings of one of the samples of malware.

**Kyberite Group**

The Kyberite Group is a series of intrusions into organizations leveraging the customer Kyberite malware. The intrusions using Kyberite are highly targeted and serve as a remote access toolkit for initial access operations. Intrusions leveraging Kyberite have been observed to see living on the land techniques internal to the victim’s network as well as the loading of custom malware that is victim specific. The Kyberite malware has been used in intrusions targeting research and development organizations as well as large scale financial theft operations and ransomware operations.

**Galactic Sentries**

The Galactic Sentries are a little known intelligence organization that prepare cyber threat intelligence reports for organizations and also are rumored to conduct cyber operations on behalf of key clients. Not much is known about them other than the fact that they were founded by Drevint Varsallas and remain a private military force to this day. There are conflicting reports on whether or not they truly engage in cyber operations or whether they are actually just a legitimate organization providing intelligence reports. Their intelligence reports have both received accolades and criticism before with their most prominent reporting ending up in court cases filed on Corellia.