April 13, 2022 17:55

The group behind PYSA ransomware has earned notoriety for targeting government agencies, educational institutions, and the healthcare sector. The group is known to carefully research high-value targets before launching its attacks, compromising enterprise systems and forcing organizations to pay large ransoms to restore their data. They are listed as one of the most advanced ransomware groups that carry out their operations off the radar.

The PRODAFT Threat Intelligence team detected and gained visibility into PYSA's ransomware infrastructure and analyzed its findings to gain insight into how the criminal operation works. The report is the first example that showcases all internal details of PYSA group, which silently carried out operations for two years.

Unlike highly automated threats that target huge numbers of victims at a time, PYSA is a highly manual ransomware operator that focuses exclusively on high-value targets. Relevant IoCs are included in the report for further research.

Organized Cyber-Crime