Indicators of Compromise (IOCs)

Indicator	Details
http://satkas.waw[.]pl/rainloop/forecast	TrailBlazer C2
1326932d63485e299ba8e03bfcd23057f7897c3ae0d26ed1235c4fb108adb105	TrailBlazer SHA256
vm-srv-1.gel.ulaval.ca	GoldMax C2
2a3b660e19b56dad92ba45dd164d300e9bd9c3b17736004878f45ee23a0177ac	GoldMax SHA256
156.96.46.116	TA Infrastructure
188.34.185.85	TA Infrastructure
212.103.61.74	TA Infrastructure
192.154.224.126	TA Infrastructure
23.29.115.180	TA Infrastructure
104.237.218.74	TA Infrastructure
23.82.128.144	TA Infrastructure