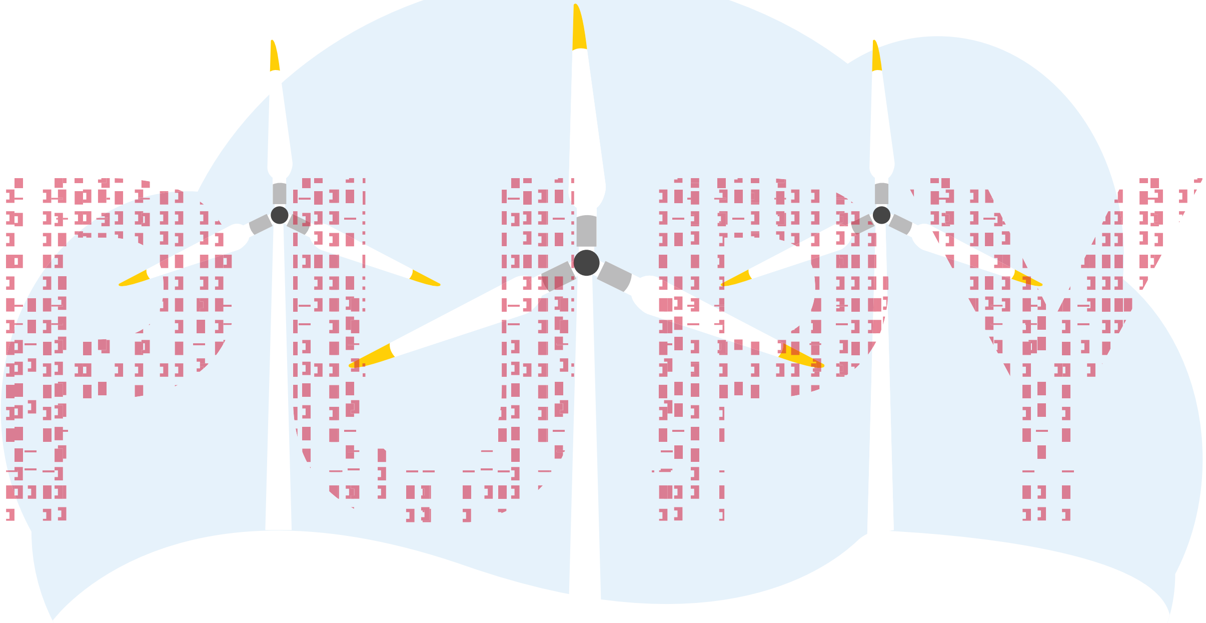
CYBER THREAT ANALYSIS

European Energy Sector Organization Targeted by PupyRAT Malware in Late 2019

By Insikt Group®



CTA-2020-0123

This report is based on proprietary Recorded Future network traffic analysis of RAT controllers detected using signatures developed by Insikt Group researchers. The period of analysis covers November 28, 2019 through January 5, 2020.

This report will primarily be of interest to SOC analysts and threat intelligence professionals in organizations operating in the energy sector who are conducting threat hunting assignments relating to malware used by Iranian nation-state threat actors.

Over the course of the last year, Recorded Future research has demonstrated that Iran-nexus groups, possibly including APT33 (also called Elfin), have been prolific in amassing operational network infrastructure throughout 2019. Additionally, in November 2019, Microsoft disclosed that APT33 had shifted focus from targeting IT networks to physical control systems used in electric utilities, manufacturing, and oil refineries. We also documented state-sponsored Iran-nexus groups making heavy use of freely available commodity malware for active network intrusions. These tools are usually intended to be used for defensive red-teaming exercises. One such tool used by several Iran-nexus groups is PupyRAT.

Using Recorded Future remote access trojan (RAT) controller detections and network traffic analysis techniques, Insikt Group identified a PupyRAT command and control (C2) server communicating with a mail server for a European energy sector organization from late November 2019 until at least January 5, 2020. While metadata alone does not confirm a compromise, we assess that the high volume and repeated communications from the targeted mail server to a PupyRAT C2 are sufficient to indicate a likely intrusion.

PupyRAT is an open source RAT available on Github, and according to the developer, it is a “cross-platform, multi-function RAT and post-exploitation tool mainly written in Python.” It has been used previously by Iranian groups APT33 (Elfin, Magic Hound, HOLMIUM) and COBALT GYPSY (which overlaps with APT34/OilRig).

Although this commodity RAT, PupyRAT, is known to have been used by Iranian threat actor groups APT33 and COBALT GYPSY, we cannot confirm whether the PupyRAT controller we identified is used by either Iranian group. Whoever the attacker is, the targeting of a mail server at a high-value critical infrastructure organization could give an adversary access to sensitive information on energy allocation and resourcing in Europe.

The targeting of a key organization in the European energy sector is of particular interest given their role in the coordination of European energy resources. Iranian groups (and others) have targeted a wide variety of industries in the U.S. and Europe, with recent reporting indicating an increase in the targeting of energy sector industrial control software.

We emphasize that this activity predates the recent escalation of kinetic activity between the U.S. and Iran, and therefore likely relates to espionage-motivated intrusion activity or the prepositioning of network access within a high-value network in the European energy sector.

To defend against commodity RATs such as PupyRAT and others, Recorded Future recommends that organizations:

- Monitor for sequential login attempts from the same IP against different accounts. This type of activity is more difficult to detect than traditional brute forcing, but will help insulate organizations from a favored tactic of cyber operators.
- Introduce multi-factor authentication. This has proven to be a highly effective mitigation practice for many organizations that have historically experienced a high level of credential stuffing and password-spraying attacks.
- Use a password manager and set a unique strong password for each online account.
- Analyze and cross-reference log data. This may help to detect incidents involving high-frequency lockouts, unsanctioned remote access attempts, temporal attack overlaps across multiple user accounts, and fingerprint unique web browser agent information.

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.