PARISITE | Dragos

dragos.com/threat/parisite

May 30, 2020

Threat Activity Group

PARISITE

Since 2017

PARISITE targets various industrial verticals including aerospace, oil and gas, and multiple utilities including water, electric, and gas. PARISITE's broad geographic targeting includes entities in the US, the Middle East, Europe, and Australia. Although PARISITE appears focused on industrial organizations with industrial control system (ICS) implementations and related entities, its targeting activity also includes government and non-governmental organizations.

Dragos identified PARISITE activity targeting ICS-related entities using known virtual private network (VPN) vulnerabilities. These vulnerabilities affect Fortinet, PulseSecure, and Palo Alto Networks VPN appliances. PARISITE's current focus of targeting vulnerable VPN appliances indicates an interest in initial access to enterprise networks, including industrial networks.

PARISITE infrastructure and capabilities date from at least 2017, indicating operations since at least that time. PARISITE uses known open source penetration testing tools for reconnaissance and to establish encrypted communications. This aligns with other activity groups increasingly using publicly available tools and resources as opposed to customized malware once achieving initial access.

At this time, PARISITE does not appear to have an ICS-specific disruptive or destructive capability, demonstrating only initial access and enabling further operations for MAGNALLIUM.

Dragos threat intelligence leverages the Dragos Platform, our threat operations center, and other sources to provide comprehensive insight into threats affecting industrial control security and safety worldwide. Dragos does not corroborate nor conduct political attribution

to threat activity. Dragos instead focuses on threat behaviors and appropriate detection and response. Read more about Dragos' approach to categorizing threat activity and attribution.

Dragos does not publicly describe ICS activity group technical details except in extraordinary circumstances in order to limit tradecraft proliferation. However, full details on PARISITE and other group tools, techniques, procedures, and infrastructure is available to network defenders via Dragos WorldView.

Contact Us For a Demo

Contact Us