



Live Webinar:

Join us Apr. 1st for a Town Hall as Robert M. Lee shares insights from his testimony before the U.S. House of Representatives Subcommittee on Cybersecurity and Infrastructure Protection.

[Register Now](#)

Dismiss Alert

[Skip to main content](#)

Dragos

Open Search

Open Menu

Products



- [Dragos Platform](#)
 - [Asset Visibility & Inventory](#)
 - [Vulnerability Management](#)
 - [Threat Detection](#)
 - [Investigation & Response](#)



- [Dragos Threat Intelligence](#)
 - [Threat Groups](#)



- [Neighborhood Keeper](#)

Services



- [Professional Services](#)
 - [Threat Hunting](#)
 - [Incident Response](#)
 - [Tabletop Exercise](#)
 - [Assessment Services](#)



- [Dragos Academy](#)

Solutions

- [By Challenge](#)

- By Industry

- [Cybersecurity Solutions](#)
- [OT Compliance](#)
- [OT Skills in IT](#)
- [ICS security roadmap](#)
- [Industrial Cyber Risk Management](#)
- [Secure Digital Transformation](#)
- [MITRE ATT&CK™ for ICS](#)
- [OT Cyber Threats](#)

By Industry

Resources



- [All Resources](#)

- [Blog](#)
- [Case Studies](#)
- [Datasheets](#)
- [Press Releases](#)
- [Reports](#)
- [Whitepapers](#)
- [Webinars](#)
- [Year In Review](#)



- [Community](#)

- [OT-CERT](#)
- [Community Defense Program](#)
- [Security Advisories](#)

Company



- [About Dragos](#)
 - [Meet the Experts](#)
 - [Why Dragos](#)
 - [Partners](#)



- [Press Releases](#)



- [Events](#)

- [DISC](#)

[Careers](#)

- [Blog](#)
- [Contact Us](#)
- [Login](#)
- [Urgent Incident Response](#)
- [Request a Demo](#)

Threat Group

RASPITE

Since 2017

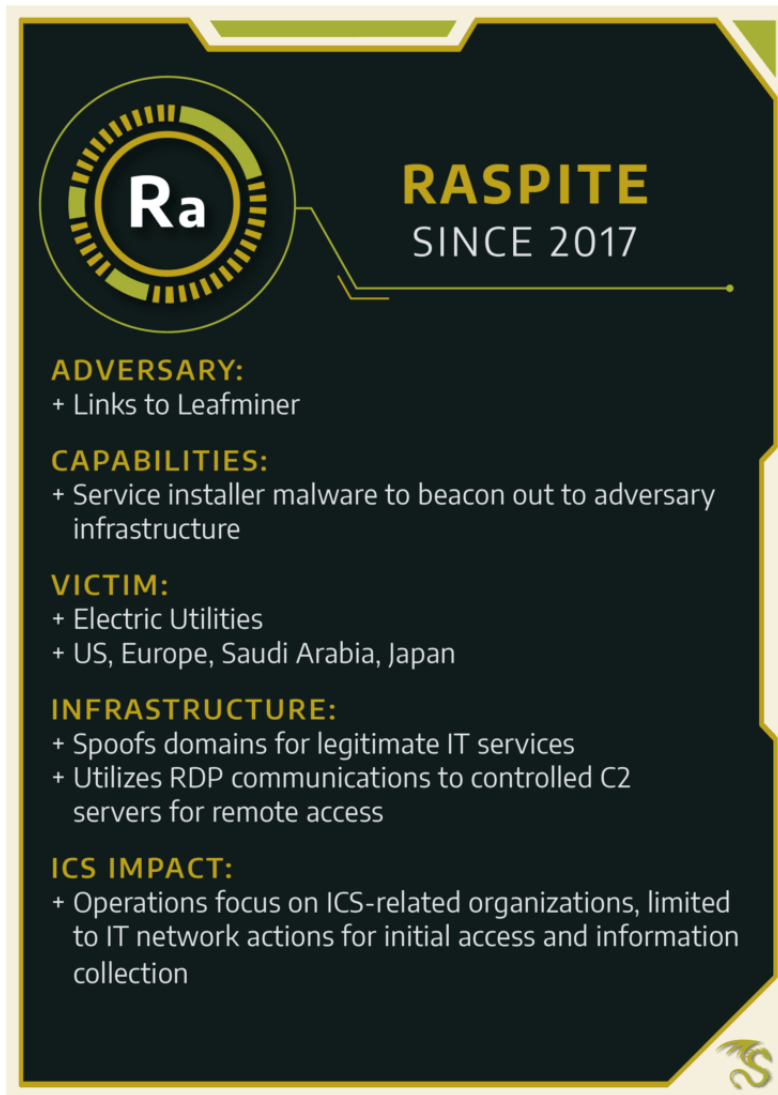
Dragos has identified a new activity group targeting access operations in the electric utility sector. We call this activity group RASPITE.

RASPITE Threat Group Operations

Analysis of RASPITE tactics, techniques, and procedures (TTPs) indicate the group has been active in some form since early- to mid-2017. RASPITE targeting includes entities in the US, Middle East, Europe, and East Asia. Operations against electric utility organizations appear limited to the US at this time.

RASPITE leverages strategic website compromise to gain initial access to target networks. RASPITE uses the same methodology as DYMALLOY and ALLANITE in embedding a link to a resource to prompt an SMB connection, from which it harvests Windows credentials. The group then deploys install scripts for a malicious service to beacon back to RASPITE-controlled infrastructure, allowing the adversary to remotely access the victim machine.

RASPITE overlaps significantly with Symantec's LEAFMINER, which recently released a report on the group's activity in the Middle East.



Ra

RASPITE
SINCE 2017

ADVERSARY:
+ Links to Leafminer

CAPABILITIES:
+ Service installer malware to beacon out to adversary infrastructure

VICTIM:
+ Electric Utilities
+ US, Europe, Saudi Arabia, Japan

INFRASTRUCTURE:
+ Spoofs domains for legitimate IT services
+ Utilizes RDP communications to controlled C2 servers for remote access

ICS IMPACT:
+ Operations focus on ICS-related organizations, limited to IT network actions for initial access and information collection

RASPITE's activity to date currently focuses on initial access operations within the electric utility sector. Although focused on ICS-operating entities, RASPITE has not demonstrated an ICS-specific capability to date. This means that the activity group is targeting electric utilities, but there is no current indication the group has the capability of destructive ICS attacks including widespread blackouts like those in Ukraine.

While the group has not yet demonstrated an ICS capability, RASPITE's recent targeting focus and methodology are clear indicators of necessary activity for initial intrusion operations into an IT network to prepare the way for later potential ICS events.

About Dragos Threat Intelligence

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 RASPITE and other group tools, techniques, procedures, and infrastructure is available to network defenders via [Dragos WorldView](#).

Contact Us For a Demo

[Contact Us](#)

[Home](#) / [Threat Groups](#) / [RASPITE](#)

Products

- [Dragos Platform](#)
- [Threat Intelligence](#)
- [Neighborhood Keeper](#)

Resources

- [Blog](#)
- [Whitepapers](#)
- [Case Studies](#)

- [Datasheets](#)
- [Webinars](#)
- [Events](#)
- [Year in Review](#)
- [Videos](#)

Company

- [About Dragos](#)
- [Careers](#)
- [Partners](#)
- [News](#)
- [DISC](#)
- [Contact Us](#)
- [Report an Incident](#)

- [Privacy Policy](#)
- [Terms of Service](#)
- [Cookies Settings](#)

- [Contact Us](#)

COPYRIGHT © 2024 DRAGOS, INC. ALL RIGHTS RESERVED.

For information about how we collect, use, share or otherwise process information about you, please see our privacy policy.

