RASPITE | Dragos

dragos.com/blog/20180802Raspite.html

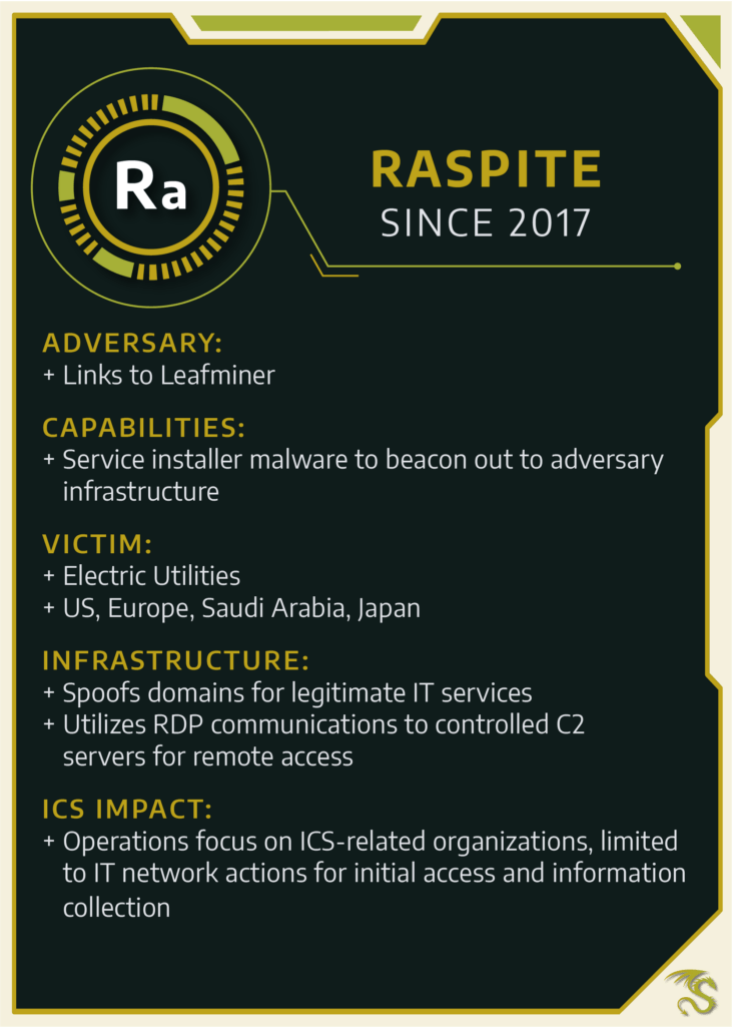
May 30, 2020

Threat Activity 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.



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.

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.

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.