# Alleged Iran-linked APT group RASPITE targets US electric utilities

August 2, 2018 By Pierluigi Paganini

**According to Dragos firm, the RASPITE cyber-espionage group (aka Leafminer) has been targeting organizations in the United States, Europe, Middle East, and East Asia.**

Researchers from security firm Dragos reported that a group operating out of Iran tracked as RASPITE has been targeting entities in the United States, Europe, Middle East, and East Asia, industrial cybersecurity firm Dragos warns.

The group has been active at least since 2017, researchers uncovered operations aimed at government and other types of organizations in the Middle East.

*"Dragos has identified a new activity group targeting access operations in the electric utility sector. We call this activity group RASPITE." read a blog post published by Dragos.*

*"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."*

Last week, experts from Symantec who tracked the group as Leafminer published a detailed report on the activity of the cyber espionage team who leveraged both custom-built malware and publicly-available tools in observed campaigns.

According to Symantec, the extent of the campaigns conducted by the group could be wider, the researchers uncovered a list, written in Iran's Farsi language, of 809 targets whose systems were scanned by the attackers.

The list groups each entry with organization of interest by geography and industry, in includes targets in the United Arab Emirates, Qatar, Bahrain, Egypt, and Afghanistan.

Now researchers from Dragos confirmed that the RASPITE is behind attacks that has been targeting industrial control systems in several states.

According to the experts, the hackers also accessed operations in the electric utility sector in the United States.

The hackers carry on watering hole attacks leveraging compromised websites providing content of interest for the potential victims.

RASPITE attacks appear similar to the ones conducted by other threat actors like DYMALLOY and ALLANITE, the hackers injected in the websites links to a resource to prompt an SMB connection with the intent to gather Windows credentials.

Then, the attackers deploy scripts to install a malware that connects to C&C ad give then attacker the control of the compromised machine.

According to Dragos, even if RASPITE has mainly focused on ICS systems, at the time there is no news about destructive attacks on such kind of devices.

*"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." continues Dragos.*

*"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."*

Sergio Caltagirone, Director of Threat Intelligence, Dragos, explained that his firm provided only limited information on the activity of the group to avoid "proliferation of ideas or tradecraft to other activity groups."

Pierluigi Paganini

(Security Affairs – RASPITE, cyber espionage)



APT | cyber espionage | Hacking | Leafminer | Pierluigi Paganini | RASPITE | Security Affairs



**Pierluigi Paganini**

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
Three members of FIN7 (Carbanak) gang charged with stealing 15 million credit cards

NEXT ARTICLE
Hundreds of thousands MikroTik Routers involved in massive Coinhive cryptomining campaign