NEWS RELEASE

Lumen Black Lotus Labs issues important report on suspected Pakistani threat actor targeting victims in South and Central Asia

2021-06-22

Actor's capabilities appear to be growing with execution of new, custom-developed framework

DENVER, June 22, 2021 /PRNewswire/ -- Black Lotus Labs, the threat intelligence arm of **Lumen** Technologies (NYSE: LUMN), today released a **detailed report** about a suspected Pakistani threat actor that executed a custom-developed framework to compromise multiple targets in South Asia, including a power company in India.

> The threat is noteworthy because of the steps it takes to avoid detection and the critical nature of the targets.

In the report, Black Lotus Labs details how it detected a new remote access trojan (RAT) it's calling ReverseRat – which was deployed in parallel with an open-source RAT called Allakore – to infect machines and achieve persistence. Based on the team's global telemetry and analysis, it determined that the actor is targeting government and energy organizations in the South and Central Asia regions, and it has operational infrastructure hosted in Pakistan.

Threat Assessment

- The ReverseRat infection chain is noteworthy because of the steps it takes to avoid detection and the critical nature of the targeted entities.
- While this threat actor's targets have thus far remained within the South and Central Asian regions, they have proven effective at gaining access to networks of interest.
- Black Lotus Labs assesses that as this actor continues to develop its capabilities and refine its multi-step infection processes, it could pose a real threat to organizations in and beyond these regions.

Black Lotus Labs Response

- To combat this campaign, Black Lotus Labs null-routed the actor's infrastructure across the Lumen global IP network and notified the affected organizations.
- Black Lotus Labs continues to follow this threat group to detect and disrupt similar compromises, and it encourages other organizations to monitor for and address this and similar campaigns in their environments.
- Black Lotus Labs is committed to tracking adversary groups such as this and documenting their tradecraft to proactively help defenders.

Recommendations
Given the nature of the critical sectors the actor is targeting and the low rate of detection, Black Lotus Labs advises security practitioners to learn the actor's current tactics, tools and procedures (TTPs) to better defend their organizations against potential attacks.

For additional IOCs such as file hashes associated with this campaign, and for this threat actor's larger activity cluster, please visit the **Black Lotus Labs blog**.

Anyone interested in collaborating on similar research can contact Black Lotus Labs on Twitter **@BlackLotusLabs**.

About Lumen Technologies:
Lumen is guided by our belief that humanity is at its best when technology advances the way we live and work. With approximately 450,000 route fiber miles and serving customers in more than 60 countries, we deliver the fastest, most secure platform for applications and data to help businesses, government and communities deliver amazing experiences.

Learn more about the Lumen network, edge cloud, security, communication and collaboration solutions and our purpose to further human progress through technology at **news.lumen.com/home**, LinkedIn: /lumentechnologies, Twitter: @lumentechco, Facebook: /lumentechnologies, Instagram: @lumentechnologies and YouTube: /lumentechnologies. Lumen and Lumen Technologies are registered trademarks in the United States.

View original content to download multimedia:**http://www.prnewswire.com/news-releases/lumen-black-lotus-labs-issues-important-report-on-suspected-pakistani-threat-actor-targeting-victims-in-south-and-central-asia-301316843.html**

SOURCE Lumen Black Lotus Labs