NEWS RELEASE

Suspected Pakistani actor modifies its custom remote access trojan with nefarious new capabilities

2021-08-11

ReverseRat 2.0 gains access to webcams and USB-connected devices while evading anti-virus detection

DENVER, Aug. 11, 2021 /PRNewswire/ -- Black Lotus Labs, the threat intelligence arm of **Lumen Technologies** (NYSE: LUMN), today announced that ReverseRat – the remote access trojan it **discovered** just six weeks ago – has been modified with **new capabilities targeting new** victims.

ReverseRat 2.0 gains access to webcams and USB-connected devices while evading anti-virus detection.

Threat Assessment

After discovering and issuing its initial ReverseRAT research, Black Lotus Labs continued to track the threat actor, which had previously targeted government and energy-sector organizations in India and Afghanistan. Some of the new discoveries include:

- Victims were lured by a .pdf file that looked like an agenda for a United Nations meeting on organized crime. The document itself appears to have been fabricated as the **UN Journal** lists no such meeting on that topic during this timeframe.
- Most of the organizations that appeared to be targeted by the new "ReverseRat 2.0" were in Afghanistan, with a handful in Jordan, India and Iran.
- The first iteration of ReverseRat relied on Allakore, an open-source RAT, to run parallel to the custom framework. ReverseRat 2.0 replaced AllaKore altogether with a new agent called NightFury.
- ReverseRat 2.0 introduced new, more intrusive capabilities including:
    - Taking photos via the infected computer's webcam and stealing files from any device connected to the compromised machine via a USB port.
    - Techniques to evade detection by Kaspersky or Quick Heal antivirus (AV) products if either were

detected on the host machine.

Black Lotus Labs Response and Recommendations

- To combat this campaign, Black Lotus Labs null-routed the threat actor 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 we encourage other organizations to alert on this and similar campaigns in their environments.
- Given the nature of the critical sectors the actor is targeting, 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.
- Anyone interested in collaborating on similar research can contact Black Lotus Labs on Twitter **@BlackLotusLabs**.

Additional Resources

- 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.**
- To catch up on Black Lotus Labs's ReverseRat research, visit the **first blog** published in June 2021.

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:**https://www.prnewswire.com/news-releases/suspected-pakistani-actor-modifies-its-custom-remote-access-trojan-with-nefarious-new-capabilities-301352897.html**

SOURCE Lumen Black Lotus Labs