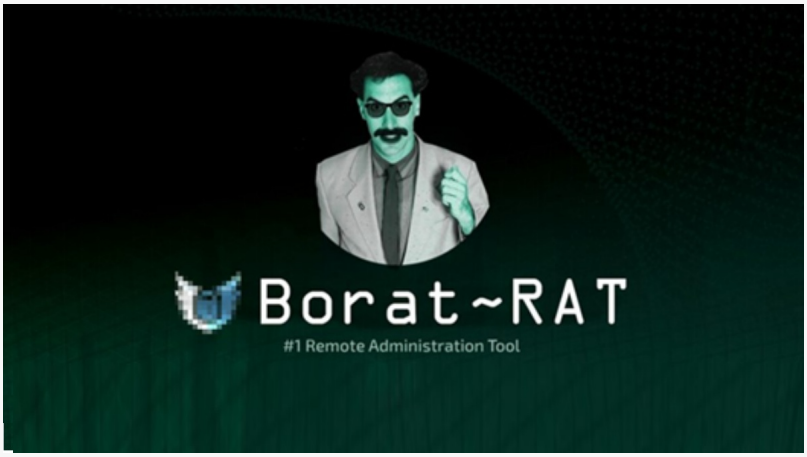
ESET Research uncovers variants of AsyncRAT, popular choice of cybercriminals



DUBAI , DUBAI, UNITED ARAB EMIRATES, July 18, 2025 /EINPresswire.com/ -- ESET Research is releasing its analysis of AsyncRAT — a remote access tool (RAT) designed to remotely monitor and control other devices. Over the years, AsyncRAT has cemented its place as a cornerstone of modern malware and as a pervasive threat that has evolved into a sprawling network of its variants and forks (customized and improved versions of the original tool). The published analysis provides an overview of the most relevant forks of AsyncRAT, drawing connections between them and showing how they have evolved.

AsyncRAT, an open-source RAT, was released on GitHub in 2019 by a user going by the name of NYAN CAT. It offers a wide range of typical RAT functionalities, including keylogging, screen capturing, credential theft, and more. Its simplicity and open-source nature have made it a popular choice among cybercriminals, leading to its widespread use in various cyberattacks.

“AsyncRAT introduced significant improvements, particularly in its modular architecture and enhanced stealth features, making it more adaptable and harder to detect in modern threat environments. Its plug-in-based architecture and ease of modification have sparked the proliferation of many forks, pushing the boundaries even further,” says ESET researcher Nikola Knežević, author of the study.

Ever since it was released to the public, AsyncRAT has spawned a multitude of new forks that have built upon its foundation. Some of these new versions have expanded on the original framework, incorporating additional features and enhancements, while others are essentially the same version in different clothes. The most popular variants for the attackers, according to ESET telemetry, are DcRat, VenomRAT, and SilverRAT.

DcRat offers a notable improvement over AsyncRAT in terms of features and capabilities, while

VenomRAT is packed with further additional features. However, not all RATs are serious in nature, and this applies equally to AsyncRAT forks. Clones like SantaRAT or BoratRAT are meant to be jokes. Despite this, ESET has found instances of real-world malicious usage of these in the wild.

In its analysis, ESET Research has cherry-picked some lesser-known forks, too, as they enhance AsyncRAT's functionality beyond the features included in the default versions. These exotic forks are often the work of one person or group, and they make up less than 1% of the volume of AsyncRAT samples.

"The widespread availability of frameworks such as AsyncRAT significantly lowers the barrier to entry for aspiring cybercriminals, enabling even novices to deploy sophisticated malware with minimal effort. This development further accelerates the creation and customization of malicious tools. This evolution underscores the importance of proactive detection strategies and deeper behavioral analyses to effectively address emerging threats," concludes Knežević.

For a more detailed analysis and technical breakdown of various AsyncRAT variants and forks, check out the latest ESET Research blogpost, "Unmasking AsyncRAT: Navigating the labyrinth of forks," on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown — securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts and blogs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

in today's world. Please see our Editorial Guidelines for more information.