RATs on the island

nimanthadeshappriya.com/post/rats-on-the-island

January 2, 2025

My commitment to keeping the Sri Lankan cybersecurity community informed continues as I explore another intriguing topic. This time, it's about **RATs**—not the rodents that are widely disliked in Sri Lanka due to their harmful effects, but rather malware known as ***Remote Access Trojans*** that cause similar damage to people, but in the digital realm.

You might wonder why I have chosen to discuss **Remote Access Trojans (RATs)** specifically, when other malware types such as stealers, botnets, banking trojans, and offensive security tools also exist. The reason for this focus is that RATs have been notably more prevalent in Sri Lanka's digital landscape compared to other malware.

My research analysed network metadata to identify RAT command-and-control (C2) servers. The findings revealed a significant increase in malicious traffic originating from Sri Lanka to these C2 channels, suggesting a concerning rise in the number of compromised individual users in the country.

In this article, I will explore what Remote Access Trojans (RATs) are, why they are prevalent, how threat actors distribute them, the techniques they use, and the most common RAT families identified in Sri Lanka's threat landscape.

A Remote Access Trojan (RAT) is a commodity malware used by threat actors to gain complete access and control over a user's system. This includes functionalities such as controlling the mouse and keyboard, accessing files, and leveraging network resources. Although RATs share similar remote-control features with legitimate tools like Remote Desktop Protocols (RDPs), they are primarily used for malicious purposes such as espionage, surveillance, and data theft. Threat actors utilize RATs to remain undetected over extended periods, enabling them to steal sensitive data, move laterally within the network, and deploy additional malware, including advanced ransomware.

RATs are prevalent globally and in Sri Lanka primarily due to two major factors: **availability** and **affordability**. Open-source RATs, such as AsyncRAT and QuasarRAT, are easily accessible to anyone and can be customized to suit specific needs. Additionally, commercially available RATs are inexpensive and can be readily purchased from underground markets or forums. The thriving malware-as-a-service (MaaS) market has further lowered entry barriers, making it easier for individuals to acquire and use these tools.

My research has identified 6 Remote Access Trojan (RAT) malware families actively present within Sri Lanka's cyber landscape. These include ***AsyncRAT***, ***Remcos RAT***, ***QuasarRAT***, ***PlugX***, ***XWorm***, and ***Orcus RAT***.

AsyncRAT stands out as the most prevalent Remote Access Trojan (RAT) in Sri Lanka's threat landscape, followed by ***Remcos RAT***. ***QuasarRAT*** ranks third but with a considerable gap in prevalence.

According to the Any.Run malware tracker, this trend has remained consistent throughout the year in Sri Lanka, with ***AsyncRAT*** and ***Remcos RAT*** being the most commonly observed malware on the platform, listed in the same order.

The first half of the year 2024 recorded relatively low malware activity, with ***Remcos RAT*** being the only malware observed during this period. However, There was a significant surge in the number of malware incidents starting in September, with ***AsyncRAT*** incidents becoming highly prevalent and ***QuasarRAT*** also making a notable appearance in the threat landscape.

Malware activities have been predominantly observed in the Western Province, particularly in the commercial city of Colombo, with a few incidents reported in other cities such as Negombo and Kaluthara. In addition, the Central Province has experienced malware incidents, especially in the major city of Kandy, while the Eastern Province has seen similar activities concentrated in Batticaloa.

This article will not delve into the technical components or provide an analysis of each malware. Instead, It will focus on how these malware families are distributed and the techniques they use. Understanding their methods of propagation and techniques is crucial

for the community to implement preventive measures and avoid becoming victims.

This article will discuss the top 3 malware observed in the Sri Lankan threat landscape, providing examples of how they are delivered to victims.

AsyncRAT

AsyncRAT is particularly noteworthy as it is an open-source tool in .NET designed for Windows systems that was released in 2019 and is still available on GitHub. This accessibility has made it one of the most commonly used RATs, both globally and in Sri Lanka. Since its initial release, ***AsyncRAT*** has been observed in numerous campaigns, often with various modifications due to its open-source nature. It has even been utilized by advanced persistent threat (APT) groups such as ***Earth Berberoka*** and ***APT-C-36***.

Research conducted by Cofense has found that HTML attachments and embedded URLs are commonly used as delivery methods. However, depending on the threat actor's modus operand, other methods may also be employed at different stages of the attack. For instance, a study by McAfee revealed that spear-phishing emails often contain a URL that downloads an HTML file with an embedded ISO file. This ISO image then contains a Windows Script File (WSF), which subsequently executes multiple files in various formats, including VBS.

The following findings are from Cofense and represent global trends, not specific to Sri Lanka.

AsyncRAT is well-equipped with various evasion techniques, including obfuscation to bypass AV/EDR, debugger evasion, and sandbox evasion, making it challenging for defense professionals to analyse. Additionally, it employs techniques such as using scheduled tasks

or registry run keys for persistence and adjusting its process token privileges with the SeDebugPrivilege token to gain elevated privileges. For more techniques, you can refer to the MITRE page dedicated to *AsyncRAT*.

AsyncRAT Techniques - MITRE ATT&CK Navigator

Remcos RAT

Unlike ***AsyncRAT***, ***Remcos RAT*** is a legitimate commercial RAT (closed-source application) sold online, designed with advanced features for remote computer control. However, its powerful and unrestricted capabilities have been exploited by threat actors to engage in malicious activities, enabling them to establish and maintain persistent, high-privileged access to victims' systems with the intent of stealing sensitive information and remotely controlling their computers. Security researchers have uncovered a vast and sophisticated ecosystem underpinning the operation of ***Remcos RAT***. This ecosystem is sustained by a network of diverse servers that act as Command and Control (C2) centers, coordinating the distribution and operation of ***Remcos RAT***.

Remcos RAT is known for employing various delivery methods and techniques throughout the different stages of an attack. However, according to Cofense, it is most commonly distributed via email, either through attachments or embedded URLs, which are also typical delivery methods for ***AsyncRAT***.

Remcos RAT is an advanced malware that shares similarities with ***AsyncRAT*** in tactics such as defense evasion, persistence, and command and control. However, it differs slightly in its techniques. For instance, ***Remcos RAT*** is known to leverage scripting languages like Python for execution and utilizes SOCKS5 proxies to enable proxying, among other distinct methods

REMCOS RAT Techniques - MITRE ATT&CK Navigator

QuasarRAT

QuasarRAT is a lightweight remote administration tool developed in C#. It is an open-source project available on GitHub. This tool offers a range of functionalities, including gathering system information, executing applications, transferring files, recording keystrokes, and capturing screenshots or webcam images.

It is worth mentioning that, unlike ***AsyncRAT*** and ***Remcos RAT***, which have been reported with specific numeric percentages for their delivery methods, the percentage distribution of delivery methods for ***QuasarRAT*** in 2024 is not readily available. However, various reports suggest that threat actors commonly use attachments and embedded URLs as delivery methods. These attachments often utilize different techniques to deliver payloads, with DLL sideloading being a notable example.

In terms of stealth, ***QuasarRAT*** does not utilize anti-analysis techniques but has been observed relying on DLL injection to evade detection in certain instances. Overall, ***QuasarRAT*** is recognized for its lower stealth capabilities while offering greater ease of use compared to ***AsyncRAT*** and ***Remcos RAT***.

QuasarRAT Techniques - MITRE ATT&CK Navigator

While other remote access trojans have been observed in Sri Lanka's threat landscape, this article focuses only on the top three, as they provide sufficient insight into how Sri Lanka has become a target for for remote access trojans. This information is valuable for cybersecurity professionals, helping them understand these attack vectors and potentially prevent falling victim, especially as malware-as-a-service continues to grow.