The Evolution of Transparent Tribe's New Malware

By gmcdouga

Published: 2024-11-04 · Archived: 2026-04-25 02:13:02 UTC

Executive Summary:

- In recent cyber attacks, Transparent Tribe, or APT36, has utilized an increasingly sophisticated malware called ElizaRAT.
- Check Point Research tracked ElizaRAT's evolution, uncovering its improved execution methods, detection evasion, and Command and Control communication since its public disclosure in September 2023.
- The ElizaRAT campaigns first executed the same function to verify that the system was set to India Standard Time, indicating that the campaigns targeted Indian systems.

Transparent Tribe, otherwise known as APT36, is a Pakistan-affiliated threat actor that notoriously targets Indian-associated entities. The threat group's main objective is cyber espionage, which has previously targeted governmental organizations, diplomatic personnel, and military facilities. Most recently, Transparent Tribe targeted Indian entities with a new malware called ElizaRAT in several successful campaigns. Since it was first detected, Check Point Research has tracked the malware, identifying increased sophistication throughout its tenure. Specifically, ElizaRAT enhanced its evasive methods and command and control capabilities.

Here, we will unravel the evolution of ElizaRAT and explain how Transparent Tribe used the increasingly advanced malware to target victims.

Background and Evolution of ElizaRAT

ElizaRAT, a Windows Remote Access Tool disclosed in September 2023, is employed by Transparent Tribe in targeted attacks. Infections typically start via executable files shared through Google Storage links, likely due to phishing efforts. Earlier variants relied on Telegram for Command and Control (C2) communication. Since its initial detection, ElizaRAT has evolved in execution methods, detection evasion, and C2 communication, as demonstrated in three distinct campaigns from late 2023 to early 2024. Each campaign utilized a different variant of ElizaRAT to deploy specific payloads for automated information gathering.

Campaign timeline, according to the malware compilation timestamps

ElizaRAT's defining characteristics include using cloud services like Google, Telegram, and Slack for distribution and C2 communication, often executed through CPL files. It employs tactics such as dropping decoy documents, creating shortcuts to the malware, and using SQLite to store victim data locally before exfiltration.

ElizaRAT Uses Slack for C2 Communication

In the first of three campaigns, a variant of ElizaRAT called Slack API used Slack channels for its C2 Communication. Created at the end of 2023, the malware is delivered as a CPL file, making it easy to run through phishing attacks. It collects user information, logs actions, checks the local time zone, and drops a fake mp4 file. The malware sends victim details to the C2 server and checks for new commands every minute. The C2 communications in the malware use Slack's API to interact with the attacker.

ApoloStealer: The New Payload

In the same campaign, transparent Tribe deployed a new payload for specific targets, which Check Point dubbed ApoloStealer. The malware was compiled one month after the ElizaRAT Slack API variant. ApoloStealer first creates a database file and then a table to store data on each file. The malware then collects its victims' desktop files. Once all relevant files are stored, ApoloStealer sends them to the C2 server.

The Circle Campaign

In January 2024, the second variant of the ElizaRAT malware called Circle was released. This version features an enhanced dropper component, significantly lowering detection rates. The Circle campaign employs a payload like Slack API's payload, though, unlike other ElizaRAT variants such as the Slack API variant, Circle avoids using cloud services for command and control (C2) and relies on a primary virtual private server (VPS) for its C2 communications.

The dropper's primary function is to prepare for ElizaRAT's execution. It extracts a zip file containing the malware and creates a working directory that places a decoy PDF and an MP4 file. The malware, just like all ElizaRAT malware, created an LNK file for the malware despite none of the malware using the file. The description of the LNK is "Slack API," which suggests a connection to the Slack campaign.

The Google Drive Campaign

Like previous versions of ElizaRAT, the third detected campaign drops the malware files, including the decoy PDF and the main ElizaRAT variant. This variant leverages Google Cloud for its C2 communication and sends commands to download the next stage payload from different virtual private servers (VPS). Check Point Research identified two payloads used in this campaign, both of which function as info stealers, each designed for a specific purpose.

Interest in India- related Targets

All ElizaRAT variants deployed the same initial function of verifying that the system's time zone was set to India Standard Time, suggesting that the campaigns targeted Indian systems.

An example of the time zone check is in the SlackFiles.dll payload. This function occurs in all samples.

As Malware Evolves, so Does Detection

The evolution of ElizaRAT demonstrates APT36's strategic efforts to refine its malware for better detection evasion and more effective targeting of Indian entities. By incorporating cloud services like Google Drive, Telegram, and Slack into its command-and-control systems, it uses widely used platforms to conceal its activities within everyday network traffic. Adding new payloads like ApolloStealer represents a significant growth in APT36's malware capabilities, indicating a shift towards a more flexible, modular approach to payload deployment. These techniques primarily focus on data collection and exfiltration, reinforcing their ongoing focus on intelligence gathering and espionage.

ElizaRAT's evolution represents threat actors' increasingly advanced tactics. Attackers become more specific and targeted, improving their campaigns' success rates and effectiveness, while enhanced evasion techniques allow for persistent activities.

To combat evolving threats, Check Point's Threat Emulation inspects all files to identify any malicious behavior before they can enter an end user's network. It recognizes unknown threats and zero-day vulnerabilities by executing files in various virtual, controlled environments, where they are monitored for harmful activity, such as unauthorized changes to the system. When integrated with Check Point Harmony Endpoint which works in real time to analyze all files, Threat Emulation evaluates each file. This process allows users to access a safe file version almost immediately while the original undergoes a more thorough inspection. This proactive approach not only enhances security by providing quick access to safe content but also ensures that potential threats are systematically identified and mitigated, thereby safeguarding the integrity of the network.

To learn more about ElizaRAT's revolution, read Check Point Research's full report.
