Severity

High

Analysis Summary

PatchWork, (also known as Mahabusa, White Elephant, hangOver, VICEROY TIGER, The Dropping Elephant) is an APT that mainly conducts cyber-espionage activities against Asian countries such as China and Pakistan. The group aims to steal sensitive information. In early July 2020, the Microstep Intelligence Bureau monitored a targeted attack with the help of the “New Coronary Pneumonia” hot event. This attack used the new crown pneumonia hot spot to deliver spear mail. Finally, the commercial Bozok remote control Trojan was loaded through the fileless loading technology to monitor the theft. Bozok RAT is a lightweight but feature-rich remote control Trojan. The client supports multiple regional languages. This Trojan has been used by many APT organizations in targeted attacks against finance and government in history. It is worth noting that in the disclosed historical attack activity of the Indian background APT organization, this attack activity is the first time they have used the Bozok Trojan. The malicious PE module released during the attack carried the digital signature certificate of Accelerate Technologies Ltd. The PE description information was the anti-software component program of the Indian security company Quick Heal. Based on this certificate, the extension line association can be associated with multiple white elephant APT attack components.

Impact

Information Theft Unauthorized Remote Access

Indicators of Compromise

MD5

- a52e4eeb2bf7f1bfdac3e3c0673ece5f

SHA-256

- 731b9ac1e4a8ddeac49a8c3c7af898fad397fb33ac9ece1dc290fc054e354ce2

SHA-1

- 6c5767a89449d934a4364dc24ce7ac609af0f26f

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.