Transparent Tribe APT actively lures Indian Army amidst increased targeting of Educational Institutions

seqrite.com/blog/transparent-tribe-apt-actively-lures-indian-army-amidst-increased-targeting-of-educational-institutions

Sathwik Ram Prakki May 2, 2023

02 May 2023

Written by Sathwik Ram Prakki

APT, Malware

Estimated reading time: 2 minutes

Overview

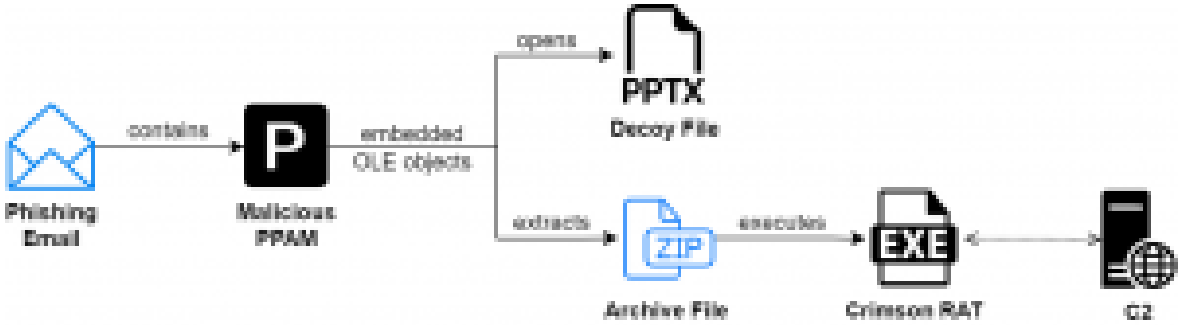
APT Transparent Tribe (APT36) is luring the Indian Army into opening the malicious file themed ‘Revision of Officers posting policy.’ Quick Heal’s APT Team has been constantly tracking this persistent threat group and has encountered a new attack campaign targeting India.

At the same time, we have also observed increased targeting of the education sector by the same threat actor. This is in continuation of targeting IITs since last year.

Furthermore, the sub-division of this group, SideCopy, has been observed recently targeting an Indian Defense Organization where the domain hosting malicious files was probably being tested to act as a phishing page.

Key Findings

- APT36 is targeting Indian Army with malicious PPAM files with ‘Officers posting policy reviseed final’ as the theme.
- These macro-enabled PowerPoint add-on files (PPAM) are utilized to wrap malicious payloads by embedding archive files as OLE objects.
- The infection chain leads to the execution of a .NET-based Crimson RAT payload that can receive and execute 22 commands along with the persistence mechanism.



Overview of Attack Chain

- C2 used by APT36 uses the same Common Name, which is usually found in this threat group’s C2 infrastructure.
- From targeting IITs to NITs and Business schools now, we have observed an increased targeting in the first quarter of 2023, peaking in February.

Summary

Transparent Tribe is a Pakistani threat group, active since 2013. It is a persistent threat actor targeting the Indian government and military entities. The group continuously uses payloads such as Crimson RAT and Capra RAT in its campaigns, constantly upgrading them.

Since May 2022 last year, Transparent Tribe has begun targeting the education sector, which surged in 2023. An in-depth analysis of the latest infection chain targeting the Indian Army and details of the education sector targeting can be found in our whitepaper.

Previous PostUnseen Threats Lurking: Protect Your Small Business from Cyberatt...

Next Post Supercharge your security operations with end-to-end visibility, ...

Sathwik Ram Prakki is working as a Security Researcher in Security Labs at Quick Heal. His focus areas are Threat Intelligence, Threat Hunting, and writing about...

Articles by Sathwik Ram Prakki »

Related Posts

- 

  Double Action, Triple Infection, and a New RAT: SideCopy's Persistent Targeting of Indian Defence

  June 15, 2023

- 

  Calling from the Underground: An alternative way to penetrate corporate networks

  January 11, 2023

- 

  Advisory on Russia-Ukraine Conflict-Related Cyberattacks

  March 15, 2022

No Comments

Leave a Reply.Your email address will not be published.