Transparent Tribe APT expands its Windows malware arsenal

blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html

By Asheer Malhotra, Justin Thattil and Kendall McKay.

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. Cisco Talos' previous research has mainly linked this group to CrimsonRAT, but new campaigns show they are expanding their Windows malware arsenal with ObliqueRAT.

While military and defense personnel continue to be the group's primary targets, Transparent Tribe is increasingly targeting diplomatic entities, defense contractors, research organizations and conference attendees, indicating that the group is expanding its targeting.

Our recent research into Transparent Tribe uncovered two types of domains the group uses in their various campaigns: fake domains masquerading as legitimate Indian defense and government-related websites, and malicious domains posing as content-hosting sites. These domains work in conjunction with each other to deliver maldocs distributing CrimsonRAT and ObliqueRAT.

Based on our findings, Transparent Tribe's tactics, techniques, and procedures (TTPs) have remained largely unchanged since 2020, but the group continues to implement new lures into its operational toolkit. The variety of maldoc lures Transparent Tribe employs indicates the group still relies on social engineering as a core component of its operations.

Hosting infrastructure

Transparent Tribe uses a two-pronged approach for registering malicious domains: Fake domains masquerading as legitimate sites belonging to government, defense, or research entities, and malicious domains that resemble file-sharing websites.

Fake domains

Our latest Transparent Tribe research confirms that the group continues to create malicious domains mimicking defense-related entities as a core component of their operations. During our most recent investigation, we discovered a fake domain, clawsindia[.]com, registered by the attackers. This domain masquerades as the website for the Center For Land Warfare Studies (CLAWS), an India-based think tank covering national security and military issues. (The legitimate domain for CLAWS is claws[.]in.) The malicious clawsindia[.]com domain was previously hosted on 164[.]68[.]101[.]194, a known command and control (C2) for CrimsonRAT, Transparent Tribe's custom .NET remote access trojan (RAT). At this point, we cannot confirm how the attackers are using or intend to use this domain as part of their broader operations. However, we also identified a subdomain, mail[.]clawsindia[.]com, hosted on the same IP, suggesting that the attackers are using it as part of a malspam campaign.

Below is one of the attackers' maldocs they used to target individuals applying for the CLAWS "Chair of Excellence," an honorary title for those making exceptional research contributions to strategic studies, according to the think tank's official documentation. The victim is encouraged to click on an embedded URL hosted on sharingmymedia[.]com, which then downloads ObliqueRAT, the trojan discovered by Talos in 2020 associated with threat activity targeting entities in South Asia.

We cannot confirm how the maldocs were delivered to victims, but we suspect they were probably sent as attachments to phishing emails based on previous threat actor behavior and the targeted nature of this particular lure. Security researchers previously discovered Transparent Tribe using sharingmymedia[.]com to host Android malware targeting Indian military and defense personnel.

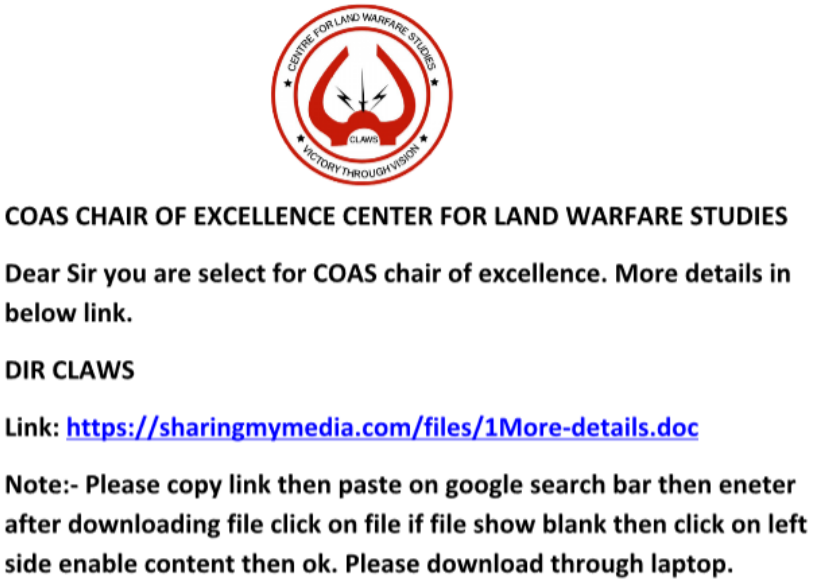


Figure 1: Maldoc masquerading as a congratulatory notice from CLAWS.

Although we could not confirm the initial infection vector of ObliqueRAT maldocs, earlier campaigns had the same infection chain as those seen in previous CrimsonRAT operations. In such cases, adversaries would deliver phishing maldocs to targets containing a malicious VBA macro that extracted either the CrimsonRAT executable or a ZIP archive embedded in the maldoc. The macro dropped the implant to the disk, setting up persistence mechanisms and eventually executing the payload on the infected endpoint.

The actors recently deviated from the CrimsonRAT infection chains to make their ObliqueRAT phishing maldocs appear more legitimate. For example, attackers leveraging ObliqueRAT started hosting their malicious payloads on compromised websites instead of embedding the malware in the maldoc. In one such case in early 2021, the adversaries used iiaonline[.]in, the Indian Industries Association's legitimate website, to host ObliqueRAT artifacts. The attackers then moved to hosting fake websites resembling those of legitimate organizations in the Indian subcontinent. Figure 2 shows the attackers' use of HTTrack, a free website copier program, to duplicate a legitimate website to use for their own malicious purposes. The attackers then used this fake website, which they hosted on a domain that was nearly identical to its legitimate counterpart, to distribute ObliqueRAT. These examples highlight Transparent Tribe's heavy reliance on social engineering as a core TTP and the group's efforts to make their operations appear as legitimate as possible.

```
<!doctype html>
<!--[if IE 7 ]><html lang="en-gb" dir="ltr" class="ie7 ltr"><![endif]-->
<!--[if IE 8 ]><html lang="en-gb" dir="ltr" class="ie8 ltr"><![endif]-->
<!--[if IE 9 ]><html lang="en-gb" dir="ltr" class="ie9 ltr"><![endif]-->
<!--[if IE 10 ]><html class="ie10"><![endif]-->
<html class="no-js" lang="en">

<!-- Mirrored from [redacted] by HTTrack Website Copier/3.x [XR&CO'2014], Fri, 29 May 2020 08:22:25 GMT -->
<!-- Added by HTTrack --><meta http-equiv="content-type" content="text/html;charset=utf-8" /><!-- /Added by HTTrack -->
<head>
```

Figure 2: Fake website cloned using HTTrack on May 29, 2020.

Another fake domain the group uses to serve CrimsonRAT is 7thcpcupdates[.]info. This domain masquerades as an information portal for The 7th Central Pay Commission (CPC) of India, which provides payment information and updates for government employees. The malicious domain prompts the victim to enter their name and email address to sign up and download a seemingly important "guide on pay and allowance."

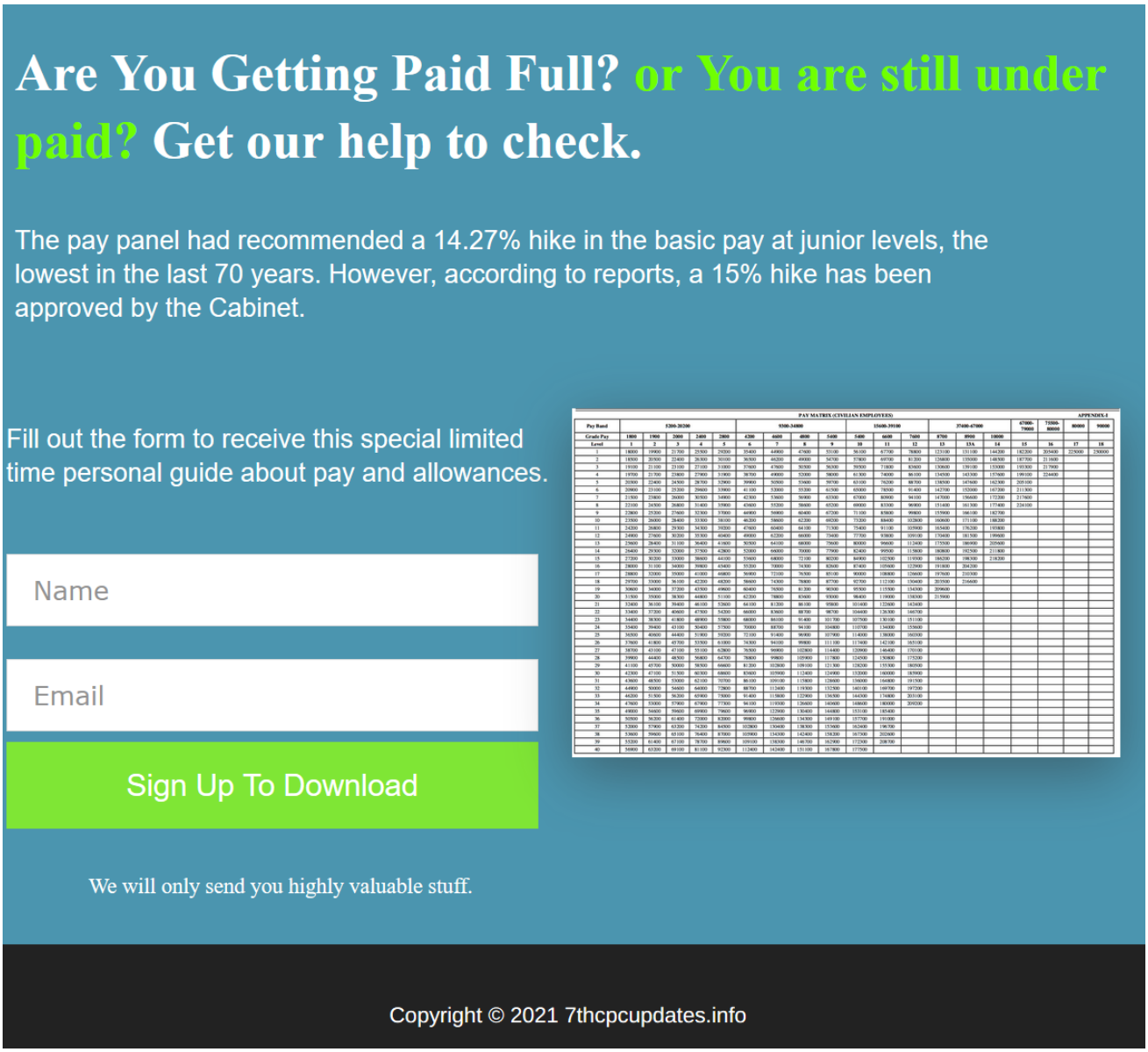


Figure 3: 7thcpcupdates[.]info landing page.

Once the victim enters their information, the portal prompts them to download the guide. Upon clicking "Download Now," a malicious XLS file is downloaded onto the victim's computer. After enabling macros, the file executes CrimsonRAT on the endpoint.

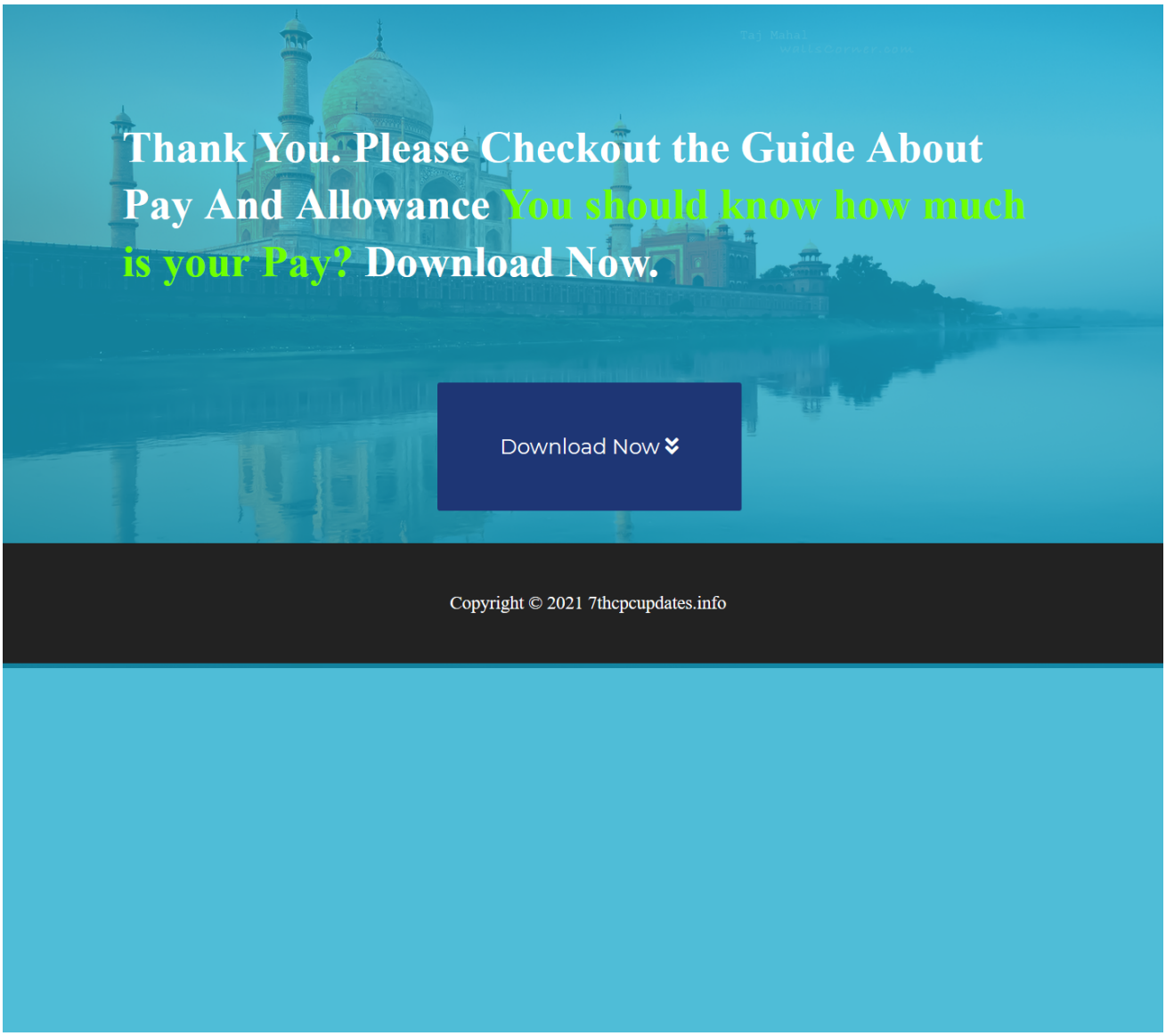


Figure 4: The "Download Now" button contains a link to a malicious XLS with CrimsonRAT embedded in it.

Malicious file-sharing domains

Transparent Tribe also regularly registers domains that appear to be legitimate file- and media-sharing services. For example, the group has used drivestransfer[.]com, file-attachment[.]com, mediaclouds[.]live, and emailhost[.]network during their operations. In the CLAWS example above, the adversaries used another such malicious domain, sharingmymedia[.]com, to host ObliqueRAT. (Additional domains are listed in the IOCs section.) The infection chain involving these domains is similar to the one described above in which the threat actors use social engineering to convince the victim to download and open the malware hosted on these sites.

Government Of India

FICCI

National Conference on Export Controls 2021

Proposed Programme

12 March, 2021 | 1500 – 1745 hrs

1430 – 1500 hrs	**Registration** **Video on Internal Compliance Programme for Effective Export Controls**
1500 – 1550 hrs	**INAUGURAL SESSION**
1500 – 1505 hrs	**Welcome Remarks** Mr Ashish Kansal, Executive Director, SMPP Pvt Ltd.*
1505 – 1515 hrs	**Export Controls as an enabler for "Make in India"** Industry Speaker
1515 -1525 hrs	**Special Remarks: Context and Relevance of Export Controls in India** Mr Sandeep Arya, JS(D&ISA), Ministry of External Affairs*
1525 – 1535 hrs	**Special Remarks: Export Controls as an accelerator for Defence Export**** Mr Sanjay Jaju, AS(DP), DDP, Ministry of Defence *
1535 – 1545 hrs	**Keynote Address:** Mr Amit Yadav, DG, Directorate General of Foreign Trade*
1545	**Release of Booklet titled 'Did You Know?'**
1545 – 1550 hrs	**Vote of Thanks** Mr. Sudhakar Gande, Co-Chairman, FICCI Defence Committee; CEO-Jupiter Capital Pvt Ltd; Non-Executive Director - AXISCADES Engineering Technologies Ltd*
1550 – 1650 hrs	**INDIA'S EXPORT CONTROL SYSTEM AND GENERAL LICENSE SCHEMES**
1550 – 1610 hrs	**India's Perspective on Export Controls** Mr Pravin Vinod, Deputy Secretary, D&ISA, MEA
1610 – 1630 hrs	**GAICT Scheme and its Benefits** Mr Sanjay Tiwari, Deputy DGFT, DGFT
1630 – 1650 hrs	**OGEL Policy** Ms Urmila Rawat, Deputy Secretary (DIP), DDP, MoD
1650 – 1745 hrs	**THEMATIC SESSION**
1650 – 1700 hrs	**Impact of Emerging Technologies on Export Controls**** Dr Anupam Srivastava, CEO of SafeZone India; Non-resident Fellow Stimson Center
1700 – 1710 hrs	**International Best Practices on General License Schemes** Ms Ameeta V. Duggal, Partner, DGS Associates*
1710 – 1720 hrs	**Need for ICP Export Compliance by industry**** Industry Speaker
1720 – 1740 hrs	**Q&A Session with Panellists**
1740 – 1745 hrs	**Concluding Remarks** FICCI

Figure 5: A sample XLS maldoc containing a malicious macro hosted on emailhost[.]network.

Lures and targeting

Transparent Tribe uses a variety of themes in their lures that evolved over time. The group has leveraged generic themes, such as resumes and CVs, since early 2019. From 2019 and continuing into 2020, the attackers started using honeytrap-themed lures to trick targets into opening ZIP archives and maldocs that posed as pictures of women. By mid-2020, the attackers reverted to primarily distributing military-themed maldocs. These maldocs did not contain popular news topics, as seen in older campaigns, but instead masqueraded as logistical and operational documents for the Indian Armed Forces.

But Transparent Tribe's attacks are not limited to only India. In one campaign, the attackers used an Iranian Ministry of Foreign Affairs (MOFA)-themed maldoc to distribute CrimsonRAT in mid-2019. Then, in mid- to late-2020, the attackers targeted diplomatic entities with RAR archives pretending to be related to the British High Commision in Islamabad, Pakistan. In mid-2020, we observed the first instance of conference attendees being targeted in the form of a CrimsonRAT maldoc masquerading as the agenda for an Afghani conference. However, since the start of this year, the group has increasingly used lures disguised as content from Indian government-sponsored conferences.

Defense-themed lures

Transparent Tribe has historically used military and defense-themes in their phishing emails and maldocs to target Indian military and government personnel. In one such case, we observed the group using the COVID-19 pandemic to target defense personnel.

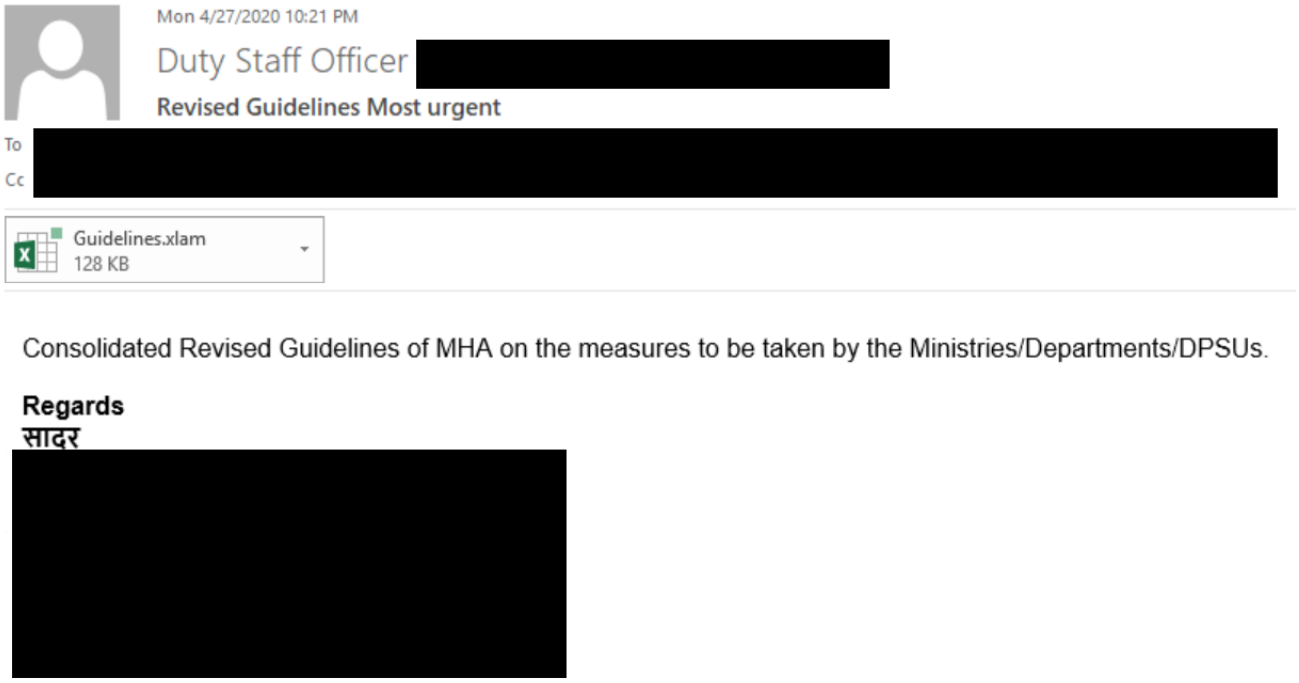


Figure 6: Transparent Tribe's spear-phishing email targeting defense personnel.

The embedded XLS maldoc masquerades as a generic Health Advisory on COVID-19. This is in line with previous reporting on Transparent Tribe's use of official COVID-19 applications and content to serve Android malware.

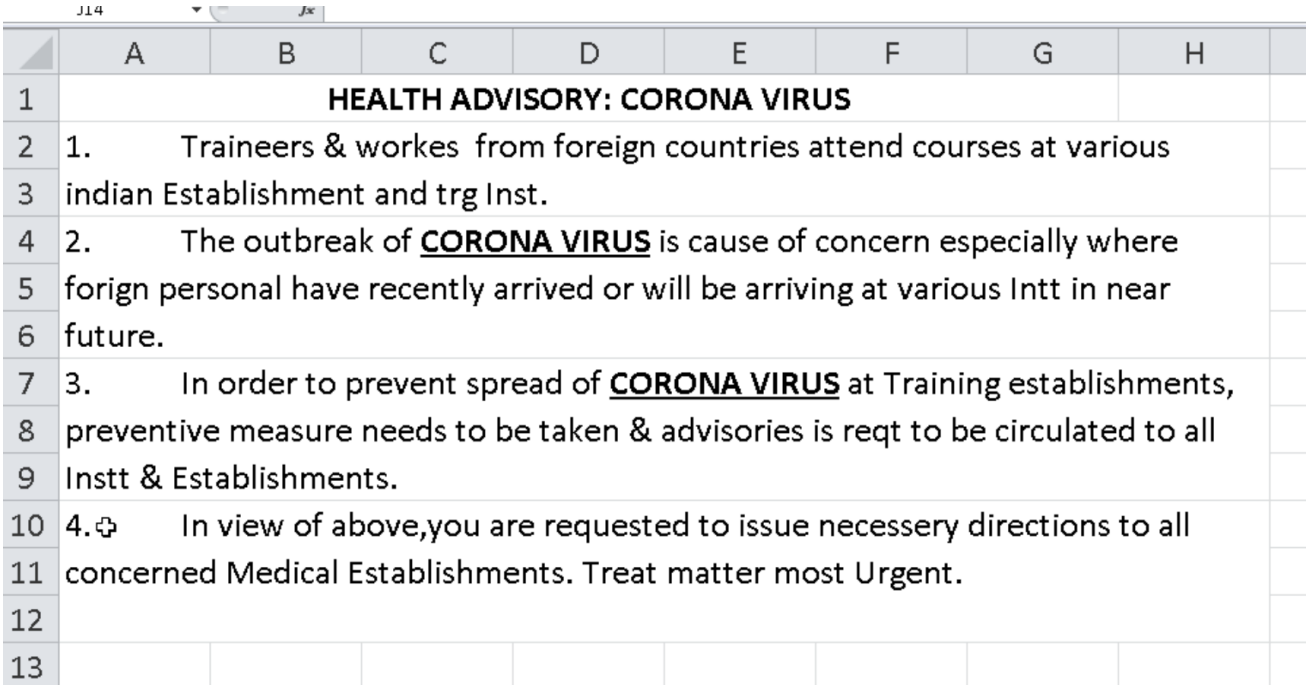


Figure 7: Attached malicious XLS macro.

Another lure targeted Indian Defense Advisors attached to various Indian embassies in Southeast Asia, as seen in Figure 8.

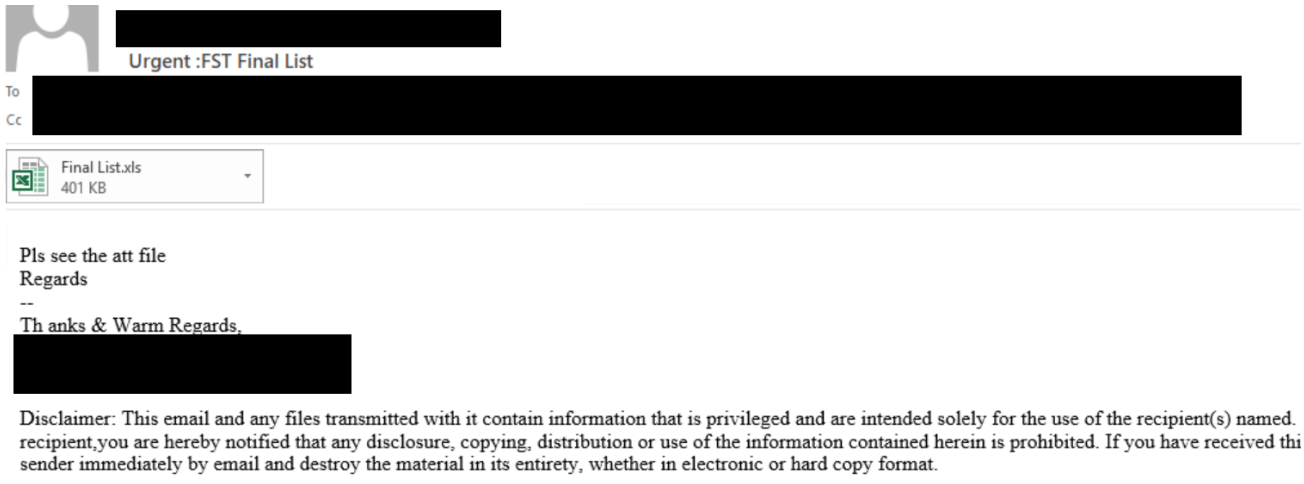


Figure 8: Spear-phishing email targeting Defense Advisors.

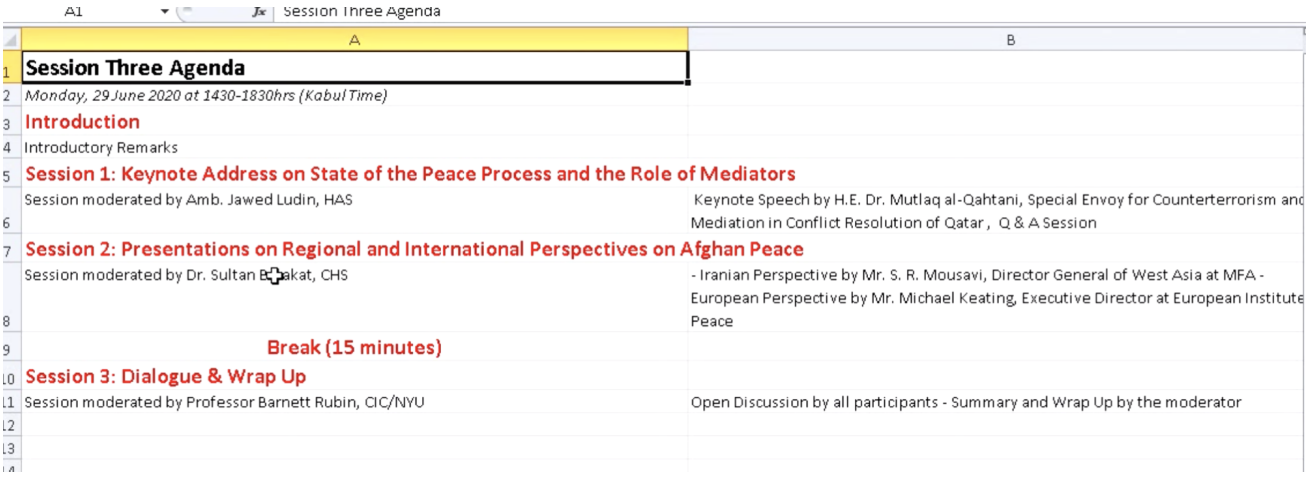
This lure consisted of a list of countries pertaining to one of the College of Defense Management's (CDM) study tours.

	A	B	C	D	E
1	**COUNTRIES TO BE VISITED DURING FOREIGN STUDY TOUR OF CDM AND THREE WAR COLLEGES**				
2	**(AWC,NWC A&CAW)**				
3	**AWC(08 GPS) 24-28 SEP**	**CAW(03 GPS) 14-18 OCT**	**NWC(02 GPS) 14-18 OCT**	**CDM(08 GPS)21-25 OCT 19**	
4	Myanmar	Japan	UK	China	
5	Germany	Russia	Singapore	UAE	
6	Canada	Turkey		South Africa	
7	Israel			Ukraine	
8	South-Korea			Malaysia	
9	Norway			France	
10	Kazakhstan			USA	
11	Nigeria			Austria	
12					
13	**Reserve**	**Reserve**	**Reserve**	**Reserve**	
14	Iran	Kazakhstan	Philippines	Chile	
15	Mauritius	Egypt	Australia	Thailand	
16	Hungry	Portugal	Greece	Denmark	
17				Maxico	
18				Kuwait	
19					

Figure 9: Maldoc impersonating a list for CDM study tours.

Conference attendees

Transparent Tribe also finds attendees of specific conferences to target. Figure 10 shows a maldoc part of a 2020 operation used to distribute CrimsonRAT. The malicious XLS contained the agenda for "Building a Peaceful Afghanistan: Regional and International Support for afghan Peace" dialogue series conducted by the Heart of Asia Society (HAS).

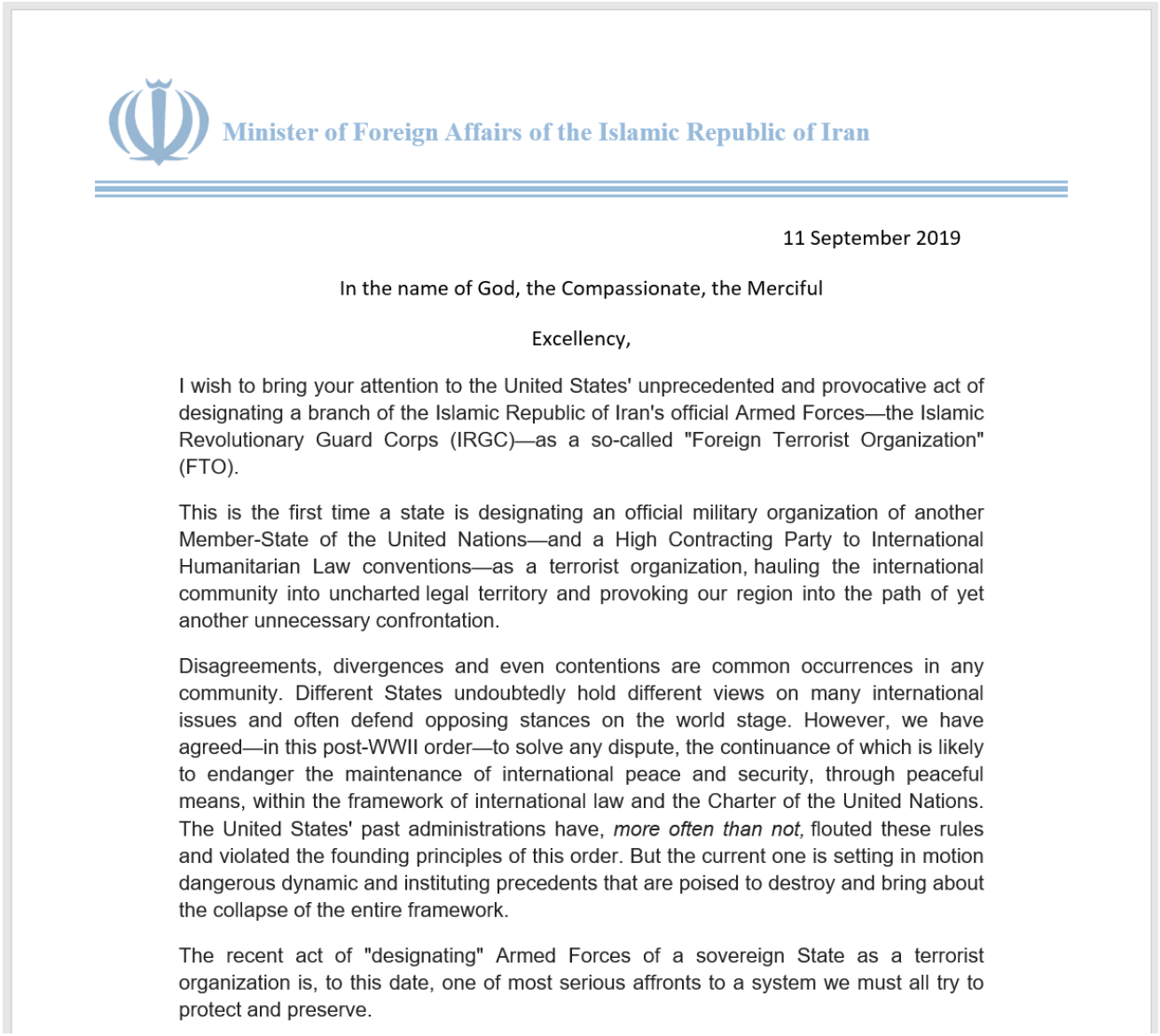


	A	B
1	**Session Three Agenda**	
2	*Monday, 29 June 2020 at 1430-1830hrs (Kabul Time)*	
3	**Introduction**	
4	Introductory Remarks	
5	**Session 1: Keynote Address on State of the Peace Process and the Role of Mediators**	
6	Session moderated by Amb. Jawed Ludin, HAS	Keynote Speech by H.E. Dr. Mutlaq al-Qahtani, Special Envoy for Counterterrorism and Mediation in Conflict Resolution of Qatar, Q & A Session
7	**Session 2: Presentations on Regional and International Perspectives on Afghan Peace**	
8	Session moderated by Dr. Sultan Barakat, CHS	- Iranian Perspective by Mr. S. R. Mousavi, Director General of West Asia at MFA - European Perspective by Mr. Michael Keating, Executive Director at European Institute Peace
9	**Break (15 minutes)**	
10	**Session 3: Dialogue & Wrap Up**	
11	Session moderated by Professor Barnett Rubin, CIC/NYU	Open Discussion by all participants - Summary and Wrap Up by the moderator
12		
13		

Figure 10: Maldoc impersonating the agenda for HAS' dialogue series 2020.

Diplomatic themes

In one incident, we observed Transparent Tribe using an Iranian-themed lure to distribute CrimsonRAT. The maldoc is a note from Iran's Foreign Minister responding to the U.S. designation of Iran's Revolutionary Guard Corps (IRGC) as a Foreign Terrorist Organization (FTO). We could not determine who the intended targets were.



Minister of Foreign Affairs of the Islamic Republic of Iran

11 September 2019

In the name of God, the Compassionate, the Merciful

Excellency,

I wish to bring your attention to the United States' unprecedented and provocative act of designating a branch of the Islamic Republic of Iran's official Armed Forces—the Islamic Revolutionary Guard Corps (IRGC)—as a so-called "Foreign Terrorist Organization" (FTO).

This is the first time a state is designating an official military organization of another Member-State of the United Nations—and a High Contracting Party to International Humanitarian Law conventions—as a terrorist organization, hauling the international community into uncharted legal territory and provoking our region into the path of yet another unnecessary confrontation.

Disagreements, divergences and even contentions are common occurrences in any community. Different States undoubtedly hold different views on many international issues and often defend opposing stances on the world stage. However, we have agreed—in this post-WWII order—to solve any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, through peaceful means, within the framework of international law and the Charter of the United Nations. The United States' past administrations have, *more often than not,* flouted these rules and violated the founding principles of this order. But the current one is setting in motion dangerous dynamic and instituting precedents that are poised to destroy and bring about the collapse of the entire framework.

The recent act of "designating" Armed Forces of a sovereign State as a terrorist organization is, to this date, one of most serious affronts to a system we must all try to protect and preserve.

Figure 11: Maldoc pretending to be a note from the MOFA Iran.

In another instance, we observed a malicious ZIP archive targeting the British High Commission in Islamabad with CrimsonRAT.

Name	Size	Packed Si...	Modified
BHC PR - British Airways Restarts Flights to Pakistan.exe	271 872	118 876	2020-08-21 16:41
British High Commission [redacted].exe	1 030 656	675 023	2020-08-21 18:14
British High Commission Press Release - GREAT Debate Islamabad 2020.exe	273 920	119 544	2020-08-21 18:15
British High Commission [redacted] receipts.exe	723 456	360 143	2020-08-21 18:16
British High Commission [redacted].exe	704 000	465 278	2020-08-21 18:17
British High Commission Urdu Press Release - GREAT Debate Islamabad 2020.exe	275 456	121 271	2020-08-21 18:17

Figure 12: Malicious archive with BHC-themed filenames containing CrimsonRAT.

HoneyTraps

Transparent Tribe consistently uses alluring documents and file names, commonly referred to as honeytraps, to trick victims into executing malicious content on their endpoints. Specifically, we have observed the group using resume documents and archives, such as ZIPs and RARs, with alluring themes distributing CrimsonRAT.

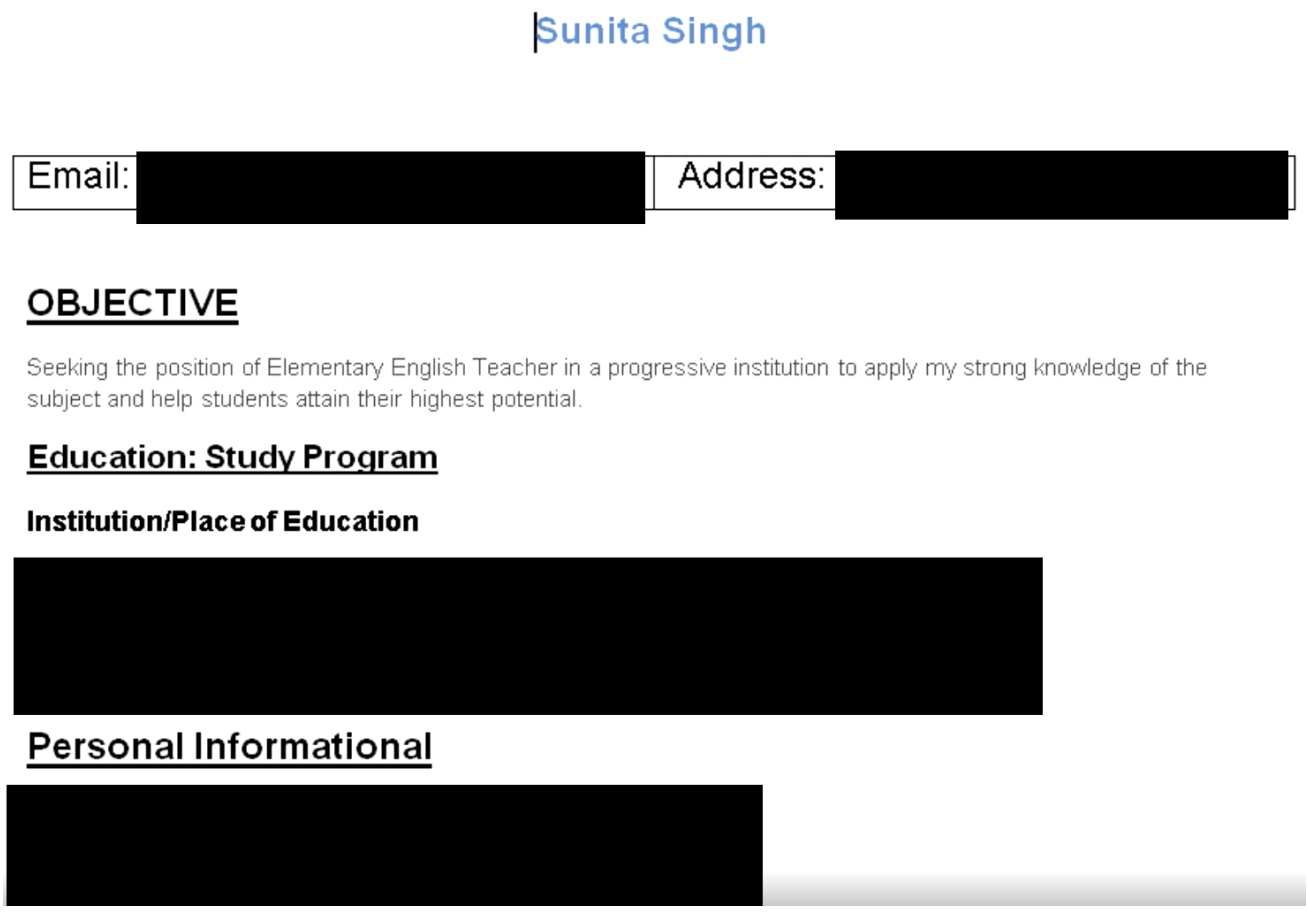


Figure 13: One of the many honeytrap lure maldocs used by Transparent Tribe.

Transparent Tribe also delivers malicious archives containing CrimsonRAT executables using various themes, including honeytraps. In a few of these instances, the malicious executables in the archives contained honeytrap-themed icons to entice the victims into executing them.

Figure 14: CrimsonRAT executables from as early as 2019 containing explicit icons.

khushi.exe

for u krishna my pic and video folder.exe

Conclusion

Transparent Tribe relies heavily on the use of maldocs to spread their Windows implants. While CrimsonRAT remains the group's staple Windows implant, their development and distribution of ObliqueRAT in early 2020 indicates they are rapidly expanding their Windows malware arsenal. Email and maldoc lures employed to spread these implants consist of multiple themes, including conference agendas, honeytrap lures and diplomatic themes. However, two common generic themes used consistently in their operations are fake resumes and military related topics. This indicates the group continues to primarily target defense personnel in the Indian subcontinent. Transparent Tribe uses generically themed content-hosting domains as well as malicious domains masquerading as legitimate defense-related websites. Coupled with the use of compromised websites to host malicious artifacts, this is evidence that the group is evolving their TTPs to appear more legitimate.

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 AMP for free here.

Cisco Secure Email can block malicious emails sent by threat actors as part of their campaign.

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 Security 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.

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

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

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

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

The following SIDs have been released to detect this threat: 57551-57562

Cisco Secure Endpoint (AMP) 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 here and here.

IOCs

A complete list of IOCs is available here.

Malicious Domains

Domains with specific themes:

- clawsindia[.]com
- mail[.]clawsindia[.]com
- larsentobro[.]com
- millitarytocorp[.]com
- 7thcpcupdates[.]info
- india[.]gov[.]in[.]attachments[.]downloads[.]7thcpcupdates[.]info
- email[.]gov[.]in[.]attachment[.]drive[.]servicesmail[.]site
- tprlink[.]com
- armypostalservice[.]com
- isroddp[.]com
- mail[.]isroddp[.]com
- pmayindia[.]com
- mailer[.]pmayindia[.]com
- mailout[.]pmayindia[.]com
- email[.]gov[.]in[.]maildrive[.]email

Generic Themed Domains:

- urservices[.]net
- drivestransfer[.]com
- emailhost[.]network
- mediaclouds[.]live
- mediabox[.]live
- mediafiles[.]live
- mediaflix[.]net
- mediadrive[.]cc
- hostflix[.]live
- shareflix[.]co
- studioflix[.]net
- social.medialinks[.]cc
- share.medialinks[.]cc
- servicesmail[.]site
- filelinks[.]live
- file-attachment[.]com
- mediashare[.]cc
- shareone[.]live
- cloudsbox[.]net
- filestudios[.]net
- datacyncorize[.]com
- templatesmanagersync[.]info
- digiphotostudio[.]live
- onedrives[.]cc
- sharingmymedia[.]com
- awsyscloud[.]com
- shareboxs[.]net
- maildrive.email
- sharemydrives[.]com
- newsupdates.myftp[.]org
- bjorn111.duckdns[.]org
- tgservermax.duckdns[.]org
- systemsupdated.duckdns[.]org
- vmd41059.contaboserver.net
- vmi433658.contaboserver.net

- tgservermax.duckdns[.]org
- micrsoft[.]ddns.net

URLs

- hxxp://drivestransfer[.]com/files/Officers-Posting-2021.doc
- hxxp://drivestransfer[.]com/files/Special-Services-Allowance-Armd-Forces.xlam
- hxxp://drivestransfer[.]com/myfiles/Dinner%20Invitation.doc/win10/Dinner%20Invitation.doc
- hxxp://drivestransfer[.]com/files/Officers-Posting-2021.doc
- hxxp://drivestransfer[.]com/files/Parade-2021.xlam
- hxxp://drivestransfer[.]com/files/Age-Review-of-Armd-Forces.doc
- hxxp://drivestransfer[.]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=IwAR1PzHnHCOjDqfpqaBqxnY401xMX6ibdgXAComUmJuHFYHgtCBHFq5NlYug
- 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
- hxxps://cloudsbox[.]net/sonam11
- hxxp://filestudios[.]net/files/Nisha%20Doc.doc
- hxxp://filestudios[.]net/
- 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/

- 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/Immediate%20Message.docm
- hxxps://7thcpcupdates[.]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[.]212.228.121
- 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