

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.



COAS CHAIR OF EXCELLENCE CENTER FOR LAND WARFARE STUDIES

Dear Sir you are select for COAS chair of excellence. More details in below link.

DIR CLAWS

Link: <https://sharingmymedia.com/files/1More-details.doc>

Note:- Please copy link then paste on google search bar then enter after downloading file click on file if file show blank then click on left side enable content then ok. Please download through laptop.

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 `iiainline[.]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.

```
3 <!doctype html>
4 <!--[if IE 7 ]><html lang="en-gb" dir="ltr" class="ie7 ltr"><![endif]-->
5 <!--[if IE 8 ]><html lang="en-gb" dir="ltr" class="ie8 ltr"><![endif]-->
6 <!--[if IE 9 ]><html lang="en-gb" dir="ltr" class="ie9 ltr"><![endif]-->
7 <!--[if IE 10 ]><html class="ie10"><![endif]-->
8 <html class="no-js" lang="en">
9
10 <!-- Mirrored from ██████████ by HTTrack Website Copier/3.x [XR&CO'2014], Fri, 29 May 2020 08:22:25 GMT -->
11 <!-- Added by HTTrack --><meta http-equiv="content-type" content="text/html; charset=utf-8" /><!-- /Added by HTTrack -->
12 <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."

Are You Getting Paid Full? or You are still under paid? Get our help to check.

The pay panel had recommended a 14.27% hike in the basic pay at junior levels, the lowest in the last 70 years. However, according to reports, a 15% hike has been approved by the Cabinet.

Fill out the form to receive this special limited time personal guide about pay and allowances.

Name

Email

Sign Up To Download

We will only send you highly valuable stuff.

Pay Band	1500-2000										2000-3000										3000-4000										4000-5000										5000-6000										6000-7000										7000-8000										8000-9000										9000-10000										10000-11000										11000-12000										12000-13000										13000-14000										14000-15000										15000-16000										16000-17000										17000-18000										18000-19000										19000-20000										20000-21000										21000-22000										22000-23000										23000-24000										24000-25000										25000-26000										26000-27000										27000-28000										28000-29000										29000-30000										30000-31000										31000-32000										32000-33000										33000-34000										34000-35000										35000-36000										36000-37000										37000-38000										38000-39000										39000-40000										40000-41000										41000-42000										42000-43000										43000-44000										44000-45000										45000-46000										46000-47000										47000-48000										48000-49000										49000-50000																																																																																																																																																																																																																																																																																																																																																																																					
	Grade Pay	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																	
Level	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
1	18000	19500	21000	22500	24000	25500	27000	28500	30000	31500	33000	34500	36000	37500	39000	40500	42000	43500	45000	46500	48000	49500	51000	52500	54000	55500	57000	58500	60000	61500	63000	64500	66000	67500	69000	70500	72000	73500	75000	76500	78000	79500	81000	82500	84000	85500	87000	88500	90000	91500	93000	94500	96000	97500	99000	100500	102000	103500	105000	106500	108000	109500	111000	112500	114000	115500	117000	118500	120000	121500	123000	124500	126000	127500	129000	130500	132000	133500	135000	136500	138000	139500	141000	142500	144000	145500	147000	148500	150000	151500	153000	154500	156000	157500	159000	160500	162000	163500	165000	166500	168000	169500	171000	172500	174000	175500	177000	178500	180000	181500	183000	184500	186000	187500	189000	190500	192000	193500	195000	196500	198000	199500	201000	202500	204000	205500	207000	208500	210000	211500	213000	214500	216000	217500	219000	220500	222000	223500	225000	226500	228000	229500	231000	232500	234000	235500	237000	238500	240000	241500	243000	244500	246000	247500	249000	250500	252000	253500	255000	256500	258000	259500	261000	262500	264000	265500	267000	268500	270000	271500	273000	274500	276000	277500	279000	280500	282000	283500	285000	286500	288000	289500	291000	292500	294000	295500	297000	298500	300000	301500	303000	304500	306000	307500	309000	310500	312000	313500	315000	316500	318000	319500	321000	322500	324000	325500	327000	328500	330000	331500	333000	334500	336000	337500	339000	340500	342000	343500	345000	346500	348000	349500	351000	352500	354000	355500	357000	358500	360000	361500	363000	364500	366000	367500	369000	370500	372000	373500	375000	376500	378000	379500	381000	382500	384000	385500	387000	388500	390000	391500	393000	394500	396000	397500	399000	400500	402000	403500	405000	406500	408000	409500	411000	412500	414000	415500	417000	418500	420000	421500	423000	424500	426000	427500	429000	430500	432000	433500	435000	436500	438000	439500	441000	442500	444000	445500	447000	448500	450000	451500	453000	454500	456000	457500	459000	460500	462000	463500	465000	466500	468000	469500	471000	472500	474000	475500	477000	478500	480000	481500	483000	484500	486000	487500	489000	490500	492000	493500	495000	496500	498000	499500	501000	502500	504000	505500	507000	508500	510000	511500	513000	514500	516000	517500	519000	520500	522000	523500	525000	526500	528000	529500	531000	532500	534000	535500	537000	538500	540000	541500	543000	544500	546000	547500	549000	550500	552000	553500	555000	556500	558000	559500	561000	562500	564000	565500	567000	568500	570000	571500	573000	574500	576000	577500	579000	580500	582000	583500	585000	586500	588000	589500	591000	592500	594000	595500	597000	598500	600000	601500	603000	604500	606000	607500	609000	610500	612000	613500	615000	616500	618000	619500	621000	622500	624000	625500	627000	628500	630000	631500	633000	634500	636000	637500	639000	640500	642000	643500	645000	646500	648000	649500	651000	652500	654000	655500	657000	658500	660000	661500	663000	664500	666000	667500	669000	670500	672000	673500	675000	676500	678000	679500	681000	682500	684000	685500	687000	688500	690000	691500	693000	694500	696000	697500	699000	700500	702000	703500	705000	706500	708000	709500	711000	712500	714000	715500	717000	718500	720000	721500	723000	724500	726000	727500	729000	730500	732000	733500	735000	736500	738000	739500	741000	742500	744000	745500	747000	748500	750000	751500	753000	754500	756000	757500	759000	760500	762000	763500	765000	766500	768000	769500	771000	772500	774000	775500	777000	778500	780000	781500	783000	784500	786000	787500	789000	790500	792000	793500	795000	796500	798000	799500	801000	802500	804000	805500	807000	808500	810000	811500	813000	814500	816000	817500	819000	820500	822000	823500	825000	826500	828000	829500	831000	832500	834000	835500	837000	838500	840000	841500	843000	844500	846000	847500	849000	850500	852000	853500	855000	856500	858000	859500	861000	862500	864000	865500	867000	868500	870000	871500	873000	874500	876000	877500	879000	880500	882000	883500	885000	886500	888000	889500	891000	892500	894000	895500	897000	898500	900000	901500	903000	904500	906000	907500	909000	910500	912000	913500	915000	916500	918000	919500	921000	922500	924000	925500	927000	928500	930000	931500	933000	934500	936000	937500	939000	940500	942000	943500	945000	946500	948000	949500	951000	952500	954000	955500	957000	958500	960000	961500	963000	964500	966000	967500	969000	970500	972000	973500	975000	976500	978000	979500	981000	982500	984000	985500	987000	988500	990000	991500	993000	994500	996000	997500	999000	1000500	1002000	1003500	1005000	1006500	1008000	1009500	1011000	1012500	1014000	1015500	1017000	1018500	1020000	1021500	1023000	1024500	1026000	1027500	1029000	1030500	1032000	1033500	1035000	1036500	1038000	1039500	1041000	1042500	1044000	1045500	1047000	1048500	1050000	1051500	1053000	1054500	1056000	1057500	1059000	1060500	1062000	1063500	1065000	1066500	1068000	1069500	1071000	1072500	1074000	1075500	1077000	1078500	1080000	1081500	1083000	1084500	1086000	1087500	1089000	1090500	1092000	1093500	1095000	1096500	1098000	1099500	1101000	1102500	1104000	1105500	1107000	1108500	1110000	1111500	1113000	1114500	1116000	1117500	1119000	1120500	1122000	1123500	1125000	1126500	1128000	1129500	1131000	1132500	1134000	1135500	1137000	1138500	1140000	1141500	1143000	1144500	1146000	1147500	1149000	1150500	1152000	1153500	1155000	1156500	1158000	1159500	1161000	1162500	1164000	1165500	1167000	1168500	1170000	1171500	1173000	1174500	1176000	1177500	1179000	1180500	1182000	1183500	1185000	1186500	1188000	1189500	1191000	1192500	1194000	1195500	1197000	1198500	1200000	1201500	1203000	1204500	1206000	1207500	1209000	1210500	1212000	1213500	1215000	1216500	1218000	1219500	1221000	1222500	1224000	1225500	1227000	1228500	1230000	1231500	1233000	1234500	1236000	1237500	1239000	1240500	1242000	1243500	1245000	1246500	1248000	1249500	1251000	1252500	1254000	1255500	1257000	1258500	1260000	1261500	1263000	1264500	1266000	1267500	1269000	1270500	1272000	1273500	1275000	1276500	1278000	1279500	1281000	1282500	1284000	1285500	1287000	1288500	1290000	1291500	1293000	1294500	1296000	1

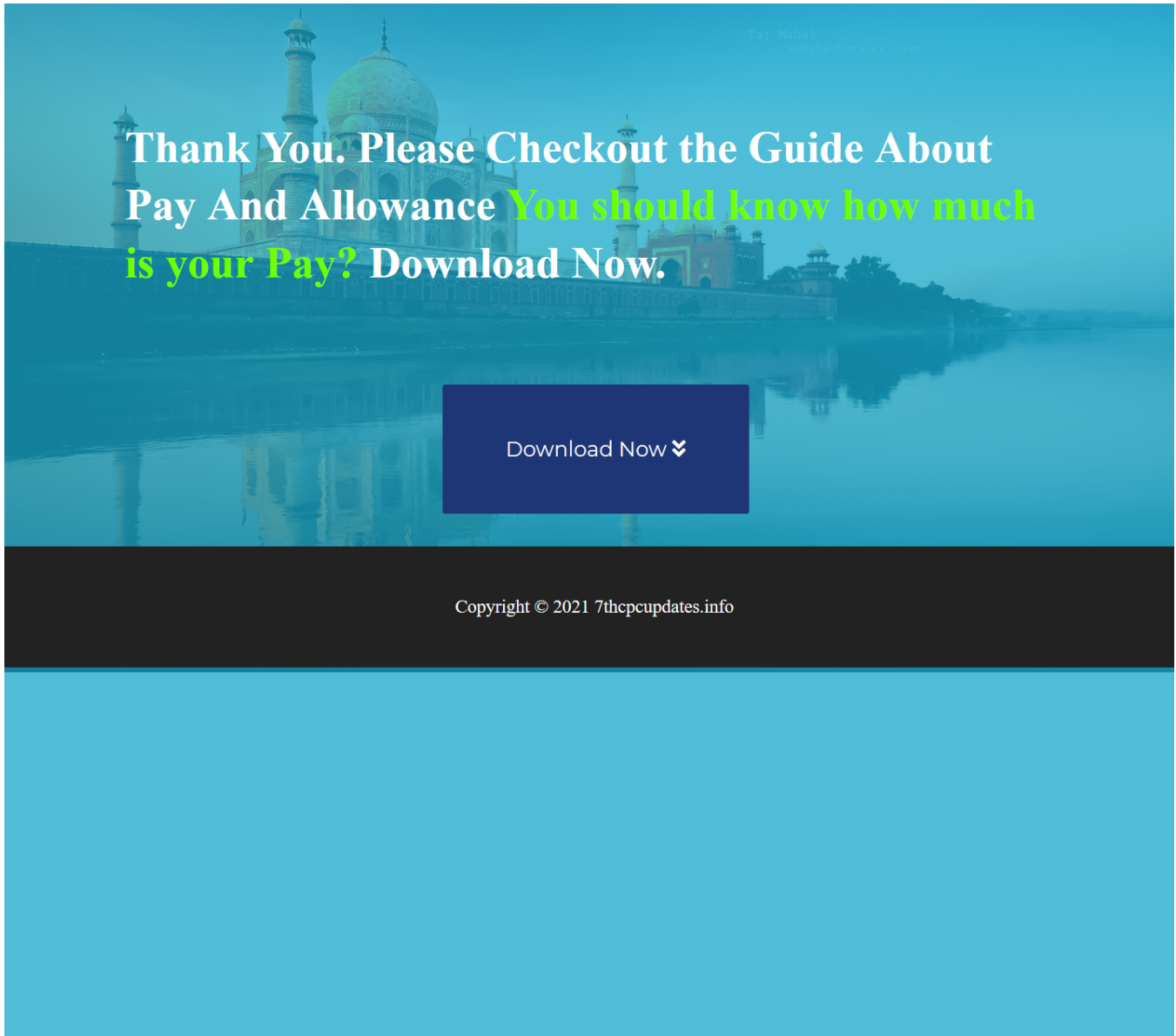


Figure 4: The "Download Now" button contains a link to a malicious XLS with CrimsonRAT embedded in it.

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 drivetransfer[.]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.



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 Commission 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.



Consolidated Revised Guidelines of MHA on the measures to be taken by the Ministries/Departments/DPSUs.

Regards
सादर

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.

	A	B	C	D	E	F	G	H
1	HEALTH ADVISORY: CORONA VIRUS							
2	1.	Trainees & workes from foreign countries attend courses at various						
3		indian Establishment and trg Inst.						
4	2.	The outbreak of <u>CORONA VIRUS</u> is cause of concern especially where						
5		foreign personal have recently arrived or will be arriving at various Intt in near						
6		future.						
7	3.	In order to prevent spread of <u>CORONA VIRUS</u> at Training establishments,						
8		preventive measure needs to be taken & advisories is reqt to be circulated to all						
9		Instt & Establishments.						
10	4.☛	In view of above,you are requested to issue necessary directions to all						
11		concerned Medical Establishments. Treat matter most Urgent.						
12								
13								

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.

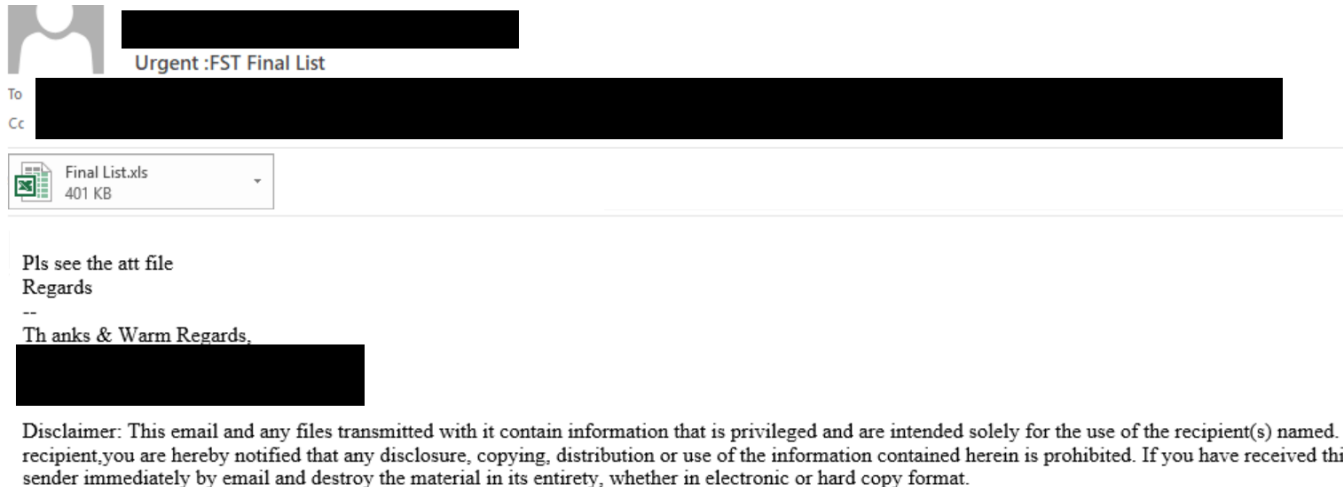


Figure 8: Spear-phishing email targeting Defense Advisors.

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	<u>COUNTRIES TO BE VISITED DURING FOREIGN STUDY TOUR OF CDM AND THREE WAR COLLEGES</u>				
2	<u>(AWC,NWC A&CAW)</u>				
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	<u>Reserve</u>	<u>Reserve</u>	<u>Reserve</u>	<u>Reserve</u>	
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	<i>Monday, 29 June 2020 at 1430-1830hrs (Kabul Time)</i>	
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 Bakat, 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		
14		

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.



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.

Email: [REDACTED] Address: [REDACTED]

OBJECTIVE

Seeking the position of Elementary English Teacher in a progressive institution to apply my strong knowledge of the subject and help students attain their highest potential.

Education: Study Program

Institution/Place of Education

[REDACTED]

Personal Informational

[REDACTED]

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.

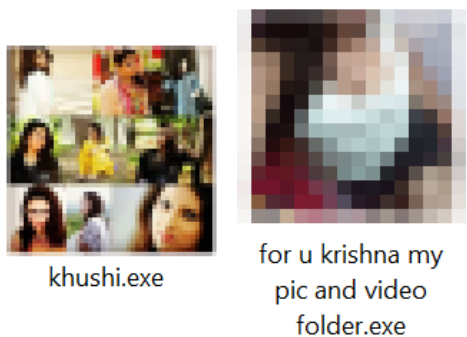


Figure 14: CrimsonRAT executables from as early as 2019 containing explicit icons.

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.

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)	✓

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.

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
- militarytocorp[.]com
- 7thpcupdates[.]info
- india[.]gov[.]in[.]attachments[.]downloads[.]7thpcupdates[.]info
- email[.]gov[.]in[.]attachment[.]drive[.]servicesmail[.]site
- tprlink[.]com
- armypostal[.]service[.]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
- datayncorize[.]com
- templatesmanagersync[.]info
- digiphotostudio[.]live
- onedrives[.]cc
- sharingmymedia[.]com
- awsyscloud[.]com
- shareboxes[.]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
- microsoft[.]ddns.net

URLs

- [http://drivestransfer\[.\]com/files/Officers-Posting-2021.doc](http://drivestransfer[.]com/files/Officers-Posting-2021.doc)
- [http://drivestransfer\[.\]com/files/Special-Services-Allowance-Armd-Forces.xlam](http://drivestransfer[.]com/files/Special-Services-Allowance-Armd-Forces.xlam)
- [http://drivestransfer\[.\]com/myfiles/Dinner%20Invitation.doc/win10/Dinner%20Invitation.doc](http://drivestransfer[.]com/myfiles/Dinner%20Invitation.doc/win10/Dinner%20Invitation.doc)
- [http://drivestransfer\[.\]com/files/Officers-Posting-2021.doc](http://drivestransfer[.]com/files/Officers-Posting-2021.doc)
- [http://drivestransfer\[.\]com/files/Parade-2021.xlam](http://drivestransfer[.]com/files/Parade-2021.xlam)
- [http://drivestransfer\[.\]com/files/Age-Review-of-Armd-Forces.doc](http://drivestransfer[.]com/files/Age-Review-of-Armd-Forces.doc)
- [http://drivestransfer\[.\]com/files/My-Resume-Detail.doc](http://drivestransfer[.]com/files/My-Resume-Detail.doc)
- [http://emailhost\[.\]network/National-Conference-2021](http://emailhost[.]network/National-Conference-2021)
- [http://mediaclouds\[.\]live/files/cnics.zip](http://mediaclouds[.]live/files/cnics.zip)
- [http://mediaclouds\[.\]live/files/attachment.zip](http://mediaclouds[.]live/files/attachment.zip)
- [http://mediabox\[.\]live/anita-resume4](http://mediabox[.]live/anita-resume4)
- [http://mediabox\[.\]live/files/nisha-resume-2020.zip](http://mediabox[.]live/files/nisha-resume-2020.zip)
- [http://mediaffles\[.\]live/files/my%20fldr%20for%20u%20diensh.zip](http://mediaffles[.]live/files/my%20fldr%20for%20u%20diensh.zip)
- [http://mediaffles\[.\]live/files/for%20u%20krishna%20my%20pic%20and%20video%20fldr.zip](http://mediaffles[.]live/files/for%20u%20krishna%20my%20pic%20and%20video%20fldr.zip)
- [http://mediaffles\[.\]live/files/khushi%20pics%20all.zip](http://mediaffles[.]live/files/khushi%20pics%20all.zip)
- [http://mediaffles\[.\]live/aditii](http://mediaffles[.]live/aditii)
- [http://mediaflix\[.\]net/BHC-PR](http://mediaflix[.]net/BHC-PR)
- [http://mediaflix\[.\]live/files/skype-lite.apk](http://mediaflix[.]live/files/skype-lite.apk)
- [http://mediadrive\[.\]cc/?a=W1549544649I](http://mediadrive[.]cc/?a=W1549544649I)
- [http://mediadrive\[.\]cc/?a=W1550558721I&fbclid=IwAR1PzHnHCOjDqfpqaBqxnY4o1xMX6ibdgXAComUmJuHFYHgtCBHFq5NIYug](http://mediadrive[.]cc/?a=W1550558721I&fbclid=IwAR1PzHnHCOjDqfpqaBqxnY4o1xMX6ibdgXAComUmJuHFYHgtCBHFq5NIYug)
- [http://hostflix\[.\]live/files/my_new_pic.zip](http://hostflix[.]live/files/my_new_pic.zip)
- [http://shareflix\[.\]co/files/lkgame.apk](http://shareflix[.]co/files/lkgame.apk)
- [http://shareflix\[.\]co/larmina-circulum-vetae-complete-2020](http://shareflix[.]co/larmina-circulum-vetae-complete-2020)
- [http://studioflix\[.\]net/my-social](http://studioflix[.]net/my-social)
- [http://social.medialinks\[.\]cc/files/scan0001.rar](http://social.medialinks[.]cc/files/scan0001.rar)
- [http://social.medialinks\[.\]cc/Case-Detail](http://social.medialinks[.]cc/Case-Detail)
- [http://social.medialinks\[.\]cc/my-100-pics](http://social.medialinks[.]cc/my-100-pics)
- [http://social.medialinks\[.\]cc/files/hot_song.rar](http://social.medialinks[.]cc/files/hot_song.rar)
- [http://email.gov.in.attachment.drive.servicesmail\[.\]site/files/Co_ast%20Guard%20HQ%2010.rar](http://email.gov.in.attachment.drive.servicesmail[.]site/files/Co_ast%20Guard%20HQ%2010.rar)
- [http://email.gov.in.attachment.drive.servicesmail\[.\]site/New-Projects-List](http://email.gov.in.attachment.drive.servicesmail[.]site/New-Projects-List)
- [http://filelinks\[.\]live/files/Note%20Verbal.doc](http://filelinks[.]live/files/Note%20Verbal.doc)
- [http://filelinks\[.\]live/Details-and-Invitations](http://filelinks[.]live/Details-and-Invitations)
- [http://file-attachment\[.\]com/files/fauji%20india%20september%202019.xls](http://file-attachment[.]com/files/fauji%20india%20september%202019.xls)
- [http://file-attachment\[.\]com/files/pfp-73rd%20independence%20day%20gallantry%20awards%20.xls](http://file-attachment[.]com/files/pfp-73rd%20independence%20day%20gallantry%20awards%20.xls)
- [http://mediashare\[.\]cc/?a=W1551315913I](http://mediashare[.]cc/?a=W1551315913I)
- [http://shareone\[.\]live/New-sonam-cv1](http://shareone[.]live/New-sonam-cv1)
- [http://cloudsbox\[.\]net/files/new%20cv.zip](http://cloudsbox[.]net/files/new%20cv.zip)
- [http://cloudsbox\[.\]net/files/new%20preet%20cv.zip](http://cloudsbox[.]net/files/new%20preet%20cv.zip)
- [http://cloudsbox\[.\]net/files/preet.doc](http://cloudsbox[.]net/files/preet.doc)
- [http://cloudsbox\[.\]net/files/sonam%20karwati.zip](http://cloudsbox[.]net/files/sonam%20karwati.zip)
- [http://cloudsbox\[.\]net/files/nisha%20arora%20sharma.zip](http://cloudsbox[.]net/files/nisha%20arora%20sharma.zip)
- [http://cloudsbox\[.\]net/files/cv%20ssss.zip](http://cloudsbox[.]net/files/cv%20ssss.zip)
- [http://cloudsbox\[.\]net/files/sonamkarwati.exe](http://cloudsbox[.]net/files/sonamkarwati.exe)
- [http://cloudsbox\[.\]net/files/sonam](http://cloudsbox[.]net/files/sonam)
- [http://cloudsbox\[.\]net/My-Pic](http://cloudsbox[.]net/My-Pic)
- [http://cloudsbox\[.\]net/files/sonam%20karwati.exe](http://cloudsbox[.]net/files/sonam%20karwati.exe)
- [http://cloudsbox\[.\]net/files/sonam](http://cloudsbox[.]net/files/sonam)
- [http://cloudsbox\[.\]net/sonam-karwati5](http://cloudsbox[.]net/sonam-karwati5)
- [http://cloudsbox\[.\]net/sonam11](http://cloudsbox[.]net/sonam11)
- [http://cloudsbox\[.\]net/sonam11](http://cloudsbox[.]net/sonam11)
- [http://filestudios\[.\]net/files/Nisha%20Doc.doc](http://filestudios[.]net/files/Nisha%20Doc.doc)
- [http://filestudios\[.\]net/](http://filestudios[.]net/)
- [http://filestudios\[.\]net/Sunita-Singh1.html](http://filestudios[.]net/Sunita-Singh1.html)
- [http://filestudios\[.\]net/files/sonam%20cv.zip](http://filestudios[.]net/files/sonam%20cv.zip)
- [http://templatesmanagersync\[.\]info/essa.dotm](http://templatesmanagersync[.]info/essa.dotm)
- [http://10feeds\[.\]com/temp.dotm](http://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://7thpcupdates[.]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