Transparent Tribe APT expands its Windows malware arsenal

By Asheer Malhotra

Published: 2021-05-13 · Archived: 2026-04-05 16:37:01 UTC

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.

<iframe src="https://open.spotify.com/embed-podcast/episode/7DqBSPHYlnhsNb2Kr1WXI5" width="100%" height="232" frameborder="0" allowtransparency="true" allow="encrypted-media"></iframe>

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.

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.

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.

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).

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.

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.

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.

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 (AMP) is ideally suited to prevent the execution of the malware detailed in this post. Below is a screenshot showing how AMP can protect customers from this threat. Try AMP for free here.

Cisco Cloud Web Security (CWS) or Cisco Secure Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

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

Network Security appliances such as Cisco Secure Firewall (NGFW), Cisco Secure IPS (NGIPS), Cisco ISR and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics helps identify malicious binaries and build protection into all Cisco Security products.

Cisco Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network.

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.

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

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=IwAR1PzHnHCOjDqfpqaBqxnY4o1xMX6ibdgXAComUmJuHFYHgtCBHFq5NlYug
- 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.
- 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

Hashes

Maldocs

662c3b181467a9d2f40a7b632a4b5fe5ddd201a528ba408badbf7b2375ee3553
9072e1af4382183be07719286f8017f6eddd9460b2e6f8a47fb042ec17aeb569

c8f27a014db8fa34fed08f6d7d50b728a8d49084dc20becdb23fff2851bae9cb

5bc32ad6ca2b8c6107c45715d61521acc0abca6f5da135161ef374f68ea3dcbd

b92890e6da84c381330319c80ec0112cba70f50ce7f9748f8a438f2c99225cd0

fb083468d19aa0ac7948c63e771890743575df1089691262fdc7963748b348a2

876939aa0aa157aa2581b74ddfc4cf03893cede542ade22a2d9ac70e2fef1656

20da161f0174d2867d2a296d4e2a8ebd2f0c513165de6f2a6f455abcecf78f2a

386ed7ba502e7bf0e60c546476c1c762cbc951eb2a2ba1f5b505be08d60310ef

67da24711012366322f2e6ab3534d62c064d24dc6e113b6077354c792cc56b71

230705996b567af8b2ed884e6c06cf2cf49a2cf5b4166a01c30d81de857627af

11c45925b64777eaa401a6c0f6a6f847fb80e82d8da8fdfe1156d28663fd9396

2f8e2c8300b7854ff204375f5116854cee7c4ef11f9b080dce89713867fd7066

6333e9f091e0f605b91d2fbae9a7040800837bdc9418ccda9bd91e894b610a20

9e305566f7d342adc8eaf30471aa3eb95c049acffc742ae23a5830a44f96e51d

cd0c624ff748d78e41c851356fbc9cc6945b426f65f64df08c7648eecc88c481

f6bec3c2d0503978f88734c6d52f2a01552c1d24b8e014ab835827ba3c9cc548

803b976d53cbb7ce9f19709f240e7a19abe82f13823d8e3ae3b44c660a957d6f

071c2ac354452d484a37e7af15dd4685061dd4af93abad4308f41df673132ff0

8bd2a1aa58cd9fb15ce499be7131e810abbdcc7770806ebfbd83b8e8f701c5e4

69f998bd67a5dbfd79bcc44f0cf2284ed61fac9bfaba3d3b4dfb19a57baa29c5

46cad0e0ca3b2d6d9d3ce691ca2887b18abc80acf0e81799fbb290cce104c8eb

74e41223ec6359a9bd05bbce36b452fd046aaad64617f459ba262a5210925942

fc3dd043b795a1cedb8b7e1e5471f15c0b5c17c237f634c60c4e0a92d980914b

d035e96f54abe59dcdbc2156e55cd0135ec420f8e97aca7f109ee8d062baa755

108a5035ab40b13b489f8a1fb8fd8bdb5880368c9c18e1d244df23b8d5a26d67

9fc84eadba969bd12cda144750cef361bcdff224026eb3921d8d46a5a424da5b

ce591810b667c31c37c856b56b277ae839a71cffe0b79e757f9105ed0208b9e4

1cb726eab6f36af73e6b0ed97223d8f063f8209d2c25bed39f010b4043b2b8a1

2aa160726037e80384672e89968ab4d2bd3b7f5ca3dfa1b9c1ecc4d1647a63f0

6c9c6966ce269bbcab164aca3c3f0231af1f7b26a18e5abc927b2ccdd9499368

d40b8c55edf7d7f118650135ee37080e8e296e635af5481e1a2850088524196c

1c2b18560f086f01541e5f2616c9faf6df4a47b878fcc2ac72ec41a7f6f30915

0335de8eadbbd5dc7cbe92ef869bcea6f6596ac39a38680142c982ec6e97ecde

856f656d41dae458a3c2a78dfa48537028b5f1e2101992dbc87bb5fe42feb821

877b64590533a9545d160acb720138d9a675a7c97dc3c48005a3edae0a44c8df

2ad362e25989b0b1911310345da90473df9053190737c456494b0c26613c8d1f

0196bc9ac3db6f02cfa97323c8fce6cc7318b8f8fadb3e73bdf7971b3c541964

b85536589c79648a10868b58075d7896ec09bbde43f9c4bad95ed82a200652bc

0196bc9ac3db6f02cfa97323c8fce6cc7318b8f8fadb3e73bdf7971b3c541964

3e9d94714c78d02eedc5f9085982edd5b840950e65702d8ee1544b643733570b

57572d520359e209357776fa2d52455dccd64999d1f3ca7a6b90bcbf11535c0a

b63f375f43a852f24f55ef3000b5a9bc3563cc5f00abcf4bea12e033348ec93b

d7317a96f983a73cdccf319bcd4461cdb736e9b6b52329278614994 94db957f2

e61aefcdeb1e5bd3855279e5e5fd676d3fdb78d1f9d6963694508e521115ea1d

6608389f584ef9dcc1ac9044965cc85400cd2f16ecff5116bb88f6320fcc6748

8afd18b6729181aa21c14ebfb869fb97c2b02099b7a832aba5d2aa22a758b694

143cd3d5e7fbbfef8a63ccee0072a47a55872bec0da514248385ead8611543c0

316b295483f59fe6b6690a3c3a889916dfb9e56375c687c48125dea601097204

dbb9168502e819619e94d9dc211d5f4967d8083ac5f4f67742b926abb04e6676

057da080ae0983585ae21195bee60d82664355a7fd78c25f21791b165c250212

dfad2a80dac91e7703266197ebbf5d67ef77467ab341dd491ad25d92d8118cac

b0ad4f3310261549c5a6cc13aadd8d7525c3cec9ef944c2b8762992360643b87

4eca66552e8c2161adf3b10eed1082f0f18b98e4526851c8da5f48d976288890

2cef1c6ead6c8faebf201a1e2b24a8e89b27e946244cf2116c607810b5e4f658

f6e7fe318a66289722770cc1786049364774464d0ff879e284b8a3fa3630e74f

6078b55381e39779f915032533a93d725bab98982b303998fa8ba2ecfc675737

0172bec4d945add9f12ce4d7d23f0e0da1ced677e89bfc132b000d444876cb41

RATs

d27474625cdc0c3456918edfa58bfaf910c8b98c6168a506ac14afc1a41fb58f

577b92a3a23917f55b1156d87ae4d4824894a3b15ae687ffa8b8af125a10438c

6ee76407efa8157b7f2b80a3a7ccc41581851aca58ab10cb8caf0243ce6fa436

10e2e486cf8ac63c12c9b50bd2e5222bc8e05b5a4d43ae2dc17dcc9ca81a78d0

d32a88349a7b10db3ba40619237009ab2fd5ec8351f3ebf3ca6865f576105a96

b67d764c981a298fa2bb14ca7faffc68ec30ad34380ad8a92911b2350104e748

17742a3ca746f7f13aff1342068b2b78df413f0c9cd6cdd02d6df7699874a13a

5a7a7c94eed3eea9fbc9ff1a32ea3422b46496e405f90858b1b169bb60bdbac6

1259ddd540300dbec4d76b5909dad475fa56b3b1837b6c7097d9b42e28d3182c

9505321807 01f8ac033a8796238d7e5b6900bc2652f28e2a44645d3cdabdeded

55a08e78689b58ba3b4bf7ea6d3a2420b15ccd7b4fccc97892b5724c538fb6c8

e3844f43afbc510d0b5c6f77e482711bbbb3dcae8e04b2f7200a11eff27c029d

e7dbf1eacfbd73576b0e410099898e4c7e2d51d76fe3095314dee1b54860bf4f

a22f6dc3eb0001c2be76d261721a1c1f419e15f6b5bfff95c5b8a5f633ce1956

c9cdd5a5b0701a4d311e0264f5bcec49fa500dde81ff8dbaa081be032b0c0446

567b82c892f10a5cc6d0286c5777e7462cec7182eba81db7dd7de53d1e8d3274

93f2358f631d4bf5a1f16b40c5bb9479dbda492d6e96c2fd9760854d219faab1

1bf6dc9af6dd730120f598d02f139f5a7776993afe29679f83a3d2fda3599736

5dcb736bf556729b30654fe97da034c1ccd7471f7587cb82dc33f4aef2248b9c

2ac34da22b6ea2d1f2c3e41c9ce01d69b16abbad9d562a238d95086c245d1762

36b57a7ff126d0f2c11e7d53d405e578dd2cda64538120dca80482c5779accdf

fe716cd97eefa66582d3a5b33b61df6760b4b6d69a68fd2bc5b2a93d6dfa11ae

9af6127a75b3cde2c5b459e5cacdd78bbfa8584dc892a93fb8b77bbb85a42731

0afb5b3572320c62a1cf10f98cea1f27ddb67fa4b8453f41c7a43faaaa48042e

c388dfa6a1e1c861c8a2301644c985d9352c43b0a41604a4385ad1a4a88fdbd3

81b67f89ebe7923e97582e3518272a49d94599107e147ff85babf231e053cf63

def8ada059c5d8017bf912990f1f9dc961c7e143822b69007411a97086f0967d

bf6705b2148f8f49bfd231de2de8939ad4686f34c0e0f6db7168be3dd8269689

706ca8e074ad04777a408b845ed56c1d675902cc2ef0aa6cca29430e967ba7af

1a8903d201f01608fba5c48f0f9d6d0546a0534c8af6fa61ecf28b2f484e77fe

6c917faa1a5ea5ae74525ace0c39c4a9208cb48f64372b8cd97c2e6e96a957db

1283da4519c11d20a9c535d2886d6e60706d62aaaa8fcdbc55eeb0ee84f9805a

0ec4af0779080f9b0b534a6b1b6f1f09ee205cf49a4334046d683d1cce84d3a0

bfcb56e41871cf6668c2699c3b0697913d0780bc0195a51ae036db7b991797d9

1fdb5dd192e813f337adc21dfe4a31e1de10bd2bbb5b58ca51a6836b7e108953

9e98fd3ad7527503b255a70ee461c02a3c9ef9aabdee3173d2f8fbb8c93d2d50

577a101dfe7db05c29570a1971e1a26e46f2f979d8ad99d51bb47665042614a5

144d8dcc78075b2f35eaf1392018127a1ff775c2a8053b91ea6837c1c246f2e2

0497e0e927adf2d0079f4e0f93dfc349bf1a2321843f8c33efe89e705900d3ba

4710d1b4feab4e2a66bb0f19f9a0b274a74ddaca72e684bf7ef8b8b9bb05e8a8

2ebcad09b11759bb64968ea3d0d73f7e6c89e21054388d80d6af9514a5d52789

7de78f7c806f828ef071a103b7be87636414635e008ea2463bf33077a466140a

d3190b5007d433e875039da72ef507a1c6e7c15cdcf7ce4409e333d89c9050ee

08b8ab37fd019b2c9d33d278eeaa16e9c50ed4c7c66ef7202eb0537ec9465a07

26e79b8af50583503b0c6bb5dc3e430ca9fdeff1e4c809ca5fea0057de7470e0

ae1ce8b298ab6c7630e20f15363c7e572fe08460bd848faef5696c883298589b

feda78f1dff8bd9d850a154a627bcfb4041dc36c325be0db436ca85fe565f767

e881c562ad195b51c9800bc32e8f170db651a7a97a9b3cc1304e80661e156c9f

b9446d663f2aef34efdb579ae02e62923b5c3bc02b9d0fe537f5974ae439a422

b01449db6a81203583e9226c5a4c4883abaeccb3fdc5bfda2d190bfeaf2d24b6

e91836bbf90b1eafd5cdcf8868408309470d4a06c5239dfee7dd74eca1a7f222

87f41a32b67c7e15827dbb83d48a7981f3d72156d61436d6b063b0429567613f

47b99e50430e9abad7326d1837ecdda5f995112b0b12406d23df5ef603d52a4e

b732193b2bbbc9c89dfd2e788a3a0f27ea54bf2868474c290fdeaa368a3a028f

3c17f3d21fddf3a1a902247d48bfbe291c2267fe7f7ce9de364ae7dff81c2eaf

ff4c5f6a1a5b68b956970751d56ee7905ec48ad39cc05416ee8ee958ecd0c40e

9ec58c011d7efbc2272a0403cd90cb4640858da7b080819737af6f1dd6b6f1e0

e4fd6452566102631a74d55b5a74b3fc5a2b7431144fb0ecf9f9fe64489a7409

be860e8882e334cd01f628e00d4e0379e7ee15468517737d3b1c984a7e4d94e8

3ce8cba4a3271721f7e2f5cab90aff56a4a6d2364d5ecbf789aa951fae7c4572

56331a4bc845b9ce0f2ad37f9c28d7c629e629d51349db0e5c5859b189c04ba1

936f2cc6458164daab71d9319cea87138f07b3845cc06ba37788c99ea5ff404a

96c730f25ee6e5a552e27b0c040f85e81a00d1c504e9f5250af60f842c6185d6

f29895d3fd197101aa284f5076a40e4e951614a7faaf214254488879b2e235f3

d0a5ffa3b9c40eb1e4277e7c41a100b0836c9424b36fb9bbe281711c0b116883

d2c46e066ff7802cecfcb7cf3bab16e63827c326b051dc61452b896a673a6e67

0283c0f02307adc4ee46c0382df4b5d7b4eb80114fbaf5cb7fe5412f027d165e

2db4365498a82081bce864196207c9478da3466167291ff7f36f93c9483fa624

682dcf03ca8d0e1af60b06820f904802f09422717d7a3d6f396a23983814e431

736b42c2f35d046855d49b4e60e25100a5a3d3fd184b0d8ac3791f79bb37419b

99b24003e4d5a19430653760db6492d920dfda94194ba8aaa9e82d2949aab740

dd47cf8ec70658af85e0cd23922462ac788305034fe78ed725bb90c1a3fa04cc

ac4214f8b674686ea5ec51946b36290367965f3f53d93a2627b5fb0ed27f6e3a

aa980e29a43487d2d6af607de7d9e3dd0b8fa0cfc3960257aec7e303e689ab56

137c059adda4df22eb29785fada54ebc00a22d150bfdc423f87ff1f6093bd827

689c049facd73d1f133f3a2aa7941f5d19ffacabf119d449643f12246a5e4d2a

87f51b4632c5fbc351a59a234dfefef506d807f2c173aac23162b85d0d73c2ad

dc31e710277eac1b125de6f4626765a2684d992147691a33964e368e5f269cba

15c45d634c70f0604cfe30806320090c66a65d8f8a26303db3c9c15bf3cc950c

e2200fa8b8c4757039e3f78536d9442817331f530e4348e08f02af753e7ae024

8b1fe0fe0a20f8ce383a2713e170f91791ee6f62915dff86fb9e070965a7be23

90175ddb90358838ea74267524d749e17a20b483b20b74d7f76fccb171226da9

68baf2a2d97213cb0d50bf9305e27c180dce6f2fd71f405143fa8f3cf775b588

fe04712df428e50a363a85db3bfe4503cad0b67449175f12a1a5eaff656348da

02e10231a6a383ff07fd6d25b3dc8dac57b077d7f27d712887a897fb6064a0c8

6f571bbee189b20d4e845e2c81d0043f9ba6141f4032a0232752e87c9549ca73

0ee399769a6e6e6d444a819ff0ca564ae584760baba93eff766926b1effe0010

e05d31b46feaa752fda5fc43dffb22bf8be669e6e3aca3ad050e42f1984b0028

e63cd1c60fd8d9f2ab6714f371958621f9d500bb09ba3569d0435f8f38960584

b4d6964b27f9090031589b2764efd1539d05eb24fe0a9330ff0f4da69725a780

a7712b7c45ae081a1576a387308077f808c666449d1ea9ba680ec410569d476f

c22c8d74daac7596b4816de5b7549927a01f65669aed7f52e382d151deb76080

425266fcaaba1204d6be8bd5e4033b6dda22d29f53c53eb88601e45d32623922

6d3982d6c6ca753d6d1daa71d88678c07718dd1919a874959a0c7975619c37fc

de1356539a38d545dd557fdb63fb1f0b3a0c348ba1570c99720cfdd59b0e2007

ca79a32fa92a7c3eb6a2997dc90410da5e1c3d8638a5e7486cad3eee3aa12fb1

20ba3c06faf0f600e0615889a4721eda75d76982b16dfdb9e4a716a46e87c0f1

152e296998d9376c13c0ea29d191e01622ddec754484b5eefd795989b8a44ab6

e5531fcf015db455a4c8fe6cb57fb5c7e179c84bb6b80194527c8ac581e055c9

777679db2c9f756a37f3092b8e3bd0c662cb05ac308f852d457c2cb71b50be96

8d537e68f562d89434f84ceb78f40fc74911b711bc1460cebf8fd1896bc9d5a2

26218ad353f0ef41ccecbd1ac0367177274422e18a98487d381be4e0741a9d6a

691d80e4b5411a15961eeacc08b6594bfa546c646301467dc31cd470d10d0191

01ec30dcacc8d6ca290ae7977bf40e07f1cb29d69ea55d2f31f41ebf5240c6ff

d70138bbb3687aa31b35ff4aadac1ffe6569de225981f299b8853bc69c0fc39e

8e1c701bcc16001a3f579ac0531187478c8b96ebc3c354f4ba170c75c33e52e0

047f76e6674abf3887162158ec0ea1de324236402fba9698cec204a2d7d8dc92

5d558a9df7802486977851c704c37ce168259df48de3cac8714b496b69da2bc8

814ed2b9ae0770d727a8cd83581b4865b2abe16f8190240c5c1e821e22a280ab

c7dbca435039a6148dc25208f04b734465e8b7c92010ede1401d88f5f8003f2d

4c21c88399d95a3602aaacf85a83c8aaac5ae7b6bf192c4c25cef4f9224b6f7b

52dee9632229ad8f163edce75e564c91b6c60c4656dafac134a4433b8d4de546

871cab3256acdbc3c27650adde878658568a85b87e85d3e3c137bdeb4592fb2c

979f7952dd2225c149f1766b4bca020b680364a77ddb6006cfa462543e0a6440

2491caddf4445d9297404493c7707b54591c989b94fd4634a7afdf54c0d22e9c

1eb0d373cea19124687ed4bffb0da3f80f98a18b9e0bebd3c12443f0a3d81689

aa6413bec5d0d549cec702430120be5bb230d36bad1a8809193ed77eea6275d6

d68ff2f6937ea8a66a68e26b41112f8db006115e7c966e28ce67029f0317992b

198871b96e9fc0bfc23204ce6a861b7fc3d9c0070e1c947cb50267dc5d454477

d4b36731cb37ad05b0b9678b568c10a56f2e84967b393b626afb19d2df41c9b9

f87d8b4376bdb341964801a836bb7ae4843351ded70801d401e951cbbe05d613

e3825a91ea1387e4247f7960afb62320a438d453df955a3ec25f590843782f38

114b6330741d974e1c97e42cff843247e7261b222ac716ea972fe59a7dfd09a1

84d9b74b7002de7f49bb7624ea63bf815497c51701bb3ec9124a0ec702178ef0

8acc17f38e5bfab577927b2477a5842517370959d35d3a80328d58bc7238e3f5

2c13ef00c1f17df9e60d650c5476e8212036c1496a7d48c85a475df5e2336ff7

2e58c371711034249cad252bbff2d49ca5ff527892ba936c007302536ff50b40

a7aae62be1b876e8bc70f963879ff7dd94427780adc8942691a3959172bdda0e

f261a7107c752cb5051c5908e9725113c1328b627388e8102f7d62731890bfe9

e507cc17eff228f9b04780e1fbef37fb7f90910cef4c32c3b9b01d3140773fdb

3f77b9266f6fe2ead71fd17f86e88ad4623023349540604a56612949808acc71

e16df177681e356ab8a9491e841fa1a757bc40069e2f42493b9238f0584cb9f1

1bdae8e9de00a8deb386f195a087f56b8b66e5c9d2b59105b6a1a3da22eb0858

8f01ae46434e75207d29bc6de069b67c350120a9880cc8e30fefc19471eaac4a

72b1b30e4b34a0267f7386974ee024c02a3b3aa62c409de18a497ca23ade20e1

3281e70706cee21cc83bdeca9eb426157898232cab366042cb84e192e58b91a4

bbea096ceb3c94454a5b92e5f614f107bd98df0b9d2f7022574256d0614f35c8

9523cf5e690302198c39e833e01f9d070f803a8445a0b40a8e33c2edc1771c3b

7afde436f24f7faceb786554857c0fef6ceefebd1be0fcd4e68542e5a2ff0c8e

a5f02bb70acdf335bed9c0fc8439ab3a220027a28c7eb44f459afda0ec7b62eb

56331a4bc845b9ce0f2ad37f9c28d7c629e629d51349db0e5c5859b189c04ba1

fd8ced785e918da29bebe5f49a909794594fec7564477d8db4aa9a170681ea39

e903e54fed007ee14305bc21219b3fab69385e4df16714d737da5953f7f3c170

497b143d5cfcda0f409ffaf51c84bd9d8e2dfdbb22500dd17420f76b4b94c55d

92717c8ecbf6524a9fefb57a346872292daa2132aeb492ccf725208474ad9179

02fddfee4928270827be0b6be617661543eb59f4a0807047eacc05c8507d188b

a7c5f87bf0a01fb12cfe8fa6da2b828e11f18ff52adbde7ee49f0b1d9ce5e40c

b658afc63bac3f28c7a70b9162480c3a8bbe7263a5f8cbb36f1430abba8fe441

bfc20b00bb5b9223db2b631061d6a5d8ba989fc5572323737a7019b9013eb89c

905fb292dc983a9d731f4716aa2e1ee289975330d11e82df95491f5a9dd7e3ed

812539ebfba481c1cde1fd4db7f523b6819e4dde7d0130f5ef60fac7de67fdb7

b2d533b84e0d3c2acc98767db3eec2888d44f12317ece1477bdb2c56e4d7a71c

15c87b1820b67d4d2b082e81fd7946dd00a1072441b7551e38fccd5575bf18c2

c57089745a418cfb8cda224fa9faf383e72df19e5bd9e1cf83f7bfd4a5c819dc

1b70f0a55b1efadd896c8b2979663f6720f702b579127a72c1c68aad259def6c

5dd8a5779aa0e2b27baf9a059f1b668323ada1da2aabe640960b518cfb1b18a3

6a8a022c8f234dd8cbbdb9f5b4dccd80fe0410652aacf0b00bf8d962f484ae37

5ba0618abff351a051f3abc3b4831376d478ca38c10e6165453c14cb3b19590f

6c85c0c30888891e6acc548af91139955b0c669181d7c2b8eaf1dd40dd3293dc

7b97b902236d07307789391174cd07de4cf4225aa1e1e738ab1a9e046a431b04

c6dbdf2978bbadb222f2f03cd745f884226472531fd7aa96bc23c55735009ff5

3945c3bd02420f6c1b0ea2b436d09f614a4389c3ebfe97f8ae17401d6c2ae925

437050e782d14bc29504ea38cd1ba01a5f6bca7b64fc80e16e241112fcb275c2

45385d371ba32d1f17b746a338fc11bb7f1acb7b66928359e1dffc7b6510051e

207397bdcd9b5818f82dc4ff9638dfee35b62b56e6e2fb7e158f13950093ac72

d17453505cada182f346b9a3033276cf509277de4a2356fbb000abf347147a7a

49def44d066cfa46fe21be29d74c0698e944f5e6911a8180aaa296d47f19366a

deeb84b07542eaa9efd4db44bf8e9ab15b9056930962352d458852410c57e3b2

6638dd6ec6c31b49c913747340fa1b2839dd9e525ac3984542669d01e8ec4ec1

e4d1f8ff1282ac60adc0134aec2420aa652250ac8ddafe866e56d2fab165a132

d2cc95b72c3e72b3888e9fa35f6fe0563f9dbbd08b76d0c3546065ceca3c5961

4b5d179531cb4baf74b8e45102c89ffe3a237bf75e80498c7982576b6557c897

1dea5c3fd77956115521e97309e5c07e220229acb142c920db996a85c018ca0e

cc8e42372ef2df10f26bc075cf3b3ca73cad573bb0eb3dfa67991e79df9d5ccd

d768aa4af126995bea32bc5cee3cad6341fc9495b47b5e20f26caa19addcacc6

b29691ac40b8bbb12b13e84641ad20583d1387ca356850aa7b5e76b0f6c76806

87bc6a307aa0a8e1a62a4bd90487653a8ce3a79239edc763875adc1b5ec60121

5a425372fac8e62d4b5d5be8054967eabe1e41894bcb8c10e431dd2e06203ca0

bdb184f4c8416c271ad2490c1165ee4d6e2efcf82a1834ba828393c74e190705

926d3f258fe2278bd1d220fafb33f246f9db9014204337f05a25d072bb644b6d

0ade4e834f34ed7693ebbe0354c668a6cb9821de581beaf1f3faae08150bd60d

4a25e48b8cf515f4cdd6711a69ccc875429dcc32007adb133fb25d63e53e2ac6

37c7500ed49671fe78bd88afa583bfb59f33d3ee135a577908d633b4e9aa4035

9da1a55b88bda3810ccd482051dc7e0088e8539ef8da5ddd29c583f593244e1c

ad17ada0171b9e619000902e62b26b949afb01b974a65258e4a7ecd59c248dba

97945ecc788f71ac05fd4eb54a41bc5704583f6928c73265dff92d4012858bad

ae24a9da37633e7812b3ce01a0716c1f0c64e0d70a9664afa04a0c1576554a74

f3148fc69a57b3b3e18ab435875ef68dac3e147d2fea4875657bf828adf09e52

887cea81fe4be74bf61a61a37d6ce93d86474ecd3fe15a0370edc672a3292cf4

48c1e890c831ce2ea0bfae2bc498f42434c1c6c9d481893fa0e57285dc3dc729

3a824bfd2a90a97365f945f965a7b2afb8a52e93a0ae4215a99a61f93aec87a1

9f6ee25ada84e57739fe3e29306bbc45b9df667bd1628e3dd1a0c2891c3deb92

e0e33f6a80bd4bab7ea7b21d64e2632d9d769aa8994ece8fae9fc358b85514d5

502c7793e4f6e5186e4ce075704b901ba053a1f99446feec4f7d16ce450880f3

108ea9a83499004c3b618a2d547bdcdd470a7012ed0eba1dcf5bdca93beb4bb3

e5570713f4ff9c3e064c136de4e0bde2b845203b1cf330db40392cc985c13cc8

07444839822a1b1a93dec11bb03e1d26444f1471eab4fd15dd0096d075ac8db7

a860ba3861df2ae0add2b695071c04468f83c0973525519d62679dd4cd4d0026

34d47a3999a36741bfb267b4429a09f0ad910b6196a298362c5cd688b2cf4d54

9b4932af4003a11929da44d1181e9c5d9414b2c510cc601accc1691d36a21649

ee84f4b188c1c76e1b98ec4821ef90bb600a3ea89c2a84ee44a1f89712565a22

59c6721a5ec5f97ef9b35e17057a5edb4f0075d1430c0cbd3eecfd44ccfe272c

8cb3a0af0bd6a9560c0eb1b197ae94542f7b479c9d3c2d9eb17ca6b9902a1959

ea4466015415499acb68e205595adf8e22a19f86097d62b9de473d4ee24a6986

ecd7d7a27a2a043919a233bb91e3b009c05b7c81ff132a7c29228e1c45d2b6a6

ecad65cf452d0f7586c8d08bc15576e5ac85ade2565e515485574cdae979bd3e

e38ff03d54d40f4e10292d7cbd614f26f3af13d01ded95dc7c363b317a5d6dd4

b5db0dd322656c19a05bc78f3ce1d8bed30e72fb8c1ac5071fce4afa720f2696

7a07fbc4903e443f237fc7c99976a8cdb751a983860ea17b891a8c617a820ad0

f26998a89d011af5860fa5c9cccf3ee09c81b14156824bdbee21e3229c7cba4b

5a449782c6d286a5af7fd5cbab5d5d46dd4dd153cbc46e4aeae0ea54f2785980

8840ac6cbd448b00849f9c84ae104a49fb3464f530cf9b2aad76f04ccb0ccc78

e60ad9543b873569432bc05cbfc8dd0f72a618f26eb256f15048b820e151846e

dfa54dc6c171740352006b7125219b1fd9cd1403be4a3440c1ad1acb1b42d37e

68253af6013d22553f3e87b8fd59dfade5c7f120b07ea679b041dcdcb845885a

aaa461c983c495c8be4bc9deaaec43ab0ce533b55e0688f6e7dbbd91f48c71b9

874501a8b8244ac00f3e2c54cbf02350c4eb7e6ce0ddeb53caff89538bc75b07

e4a91f80d9a84e6efa7fe6664075c04f1953dec5fc4177a4e8187e4d01888148

11ae7e7ab4d36dfe0bc33fd7719eaea5acd0ecbe17b32943660acb7647c33c34

9f5265056373d64e816c502cc3018550b3dea1ae4eae081b0631242a29a74faf

bccfcbb8097dd32f0870621fa6d33f993f2d180a874eccc69b97815f3052d5c1

Associated Malicious Email IDs

pmaymis-mhupa[at]pmayindia[]com

vikaskumar[.]patel[at]larsentobro[.]com

larsento[at]larsentobro[.]com
