


CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®

CTA-CN-2021-0228



China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions



This report details a campaign conducted by a China-linked threat activity group, RedEcho, targeting the Indian power sector. The activity was identified through a combination of large-scale automated network traffic analytics and expert analysis. Data sources include the Recorded Future Platform, SecurityTrails, Spur, Farsight, and common open-source tools and techniques. The report will be of most interest to individuals engaged in strategic and operational intelligence relating to Indian and Chinese activity in cyberspace.

Recorded Future notified the appropriate Indian government departments prior to publication of the suspected intrusions to support incident response and remediation investigations within the impacted organizations.

Executive Summary

Relations between India and China have deteriorated significantly following border clashes in May 2020 that resulted in the [first combat deaths](#) in 45 years between the world's two most populous nations. As a result, on January 12, 2021, India's foreign minister Subrahmanyam Jaishankar [announced](#) that trust between India and China was "profoundly disturbed." While diplomacy and economic factors have been effective in preventing a full-blown war, notable most recently with the [bilateral disengagement](#) at the border, cyber operations continue to provide countries with a potent asymmetric capability to conduct espionage or pre-position within networks for potentially disruptive reasons.

Since early 2020, Recorded Future's Insikt Group observed a large increase in suspected targeted intrusion activity against Indian organizations from Chinese state-sponsored groups. From mid-2020 onwards, Recorded Future's midpoint collection revealed a steep rise in the use of infrastructure tracked as AXIOMATICASYMPTOTE, which encompasses ShadowPad command and control (C2) servers, to target a large swathe of India's power sector. 10 distinct Indian power sector organizations, including 4 of the 5 Regional Load Despatch Centres (RLDC) responsible for operation of the power grid through balancing electricity supply and demand, have been identified as targets in a concerted campaign against India's critical infrastructure. Other targets identified included 2 Indian seaports.

Using a combination of proactive adversary infrastructure detections, domain analysis, and Recorded Future Network Traffic Analysis, we have determined that a subset of these AXIOMATICASYMPTOTE servers share some common infrastructure tactics, techniques, and procedures (TTPs) with several previously reported Chinese state-sponsored groups, including [APT41](#) and Tonto Team.

Despite some overlaps with previous groups, Insikt Group does not currently believe there is enough evidence to firmly attribute the activity in this particular campaign to an existing public group and therefore continue to track it as a closely related but distinct activity group, RedEcho.

Key Judgments

- The targeting of Indian critical infrastructure offers limited economic espionage opportunities; however, we assess they pose significant concerns over potential pre-positioning of network access to support Chinese strategic objectives.
- Pre-positioning on energy assets may support several potential outcomes, including geo-strategic signaling during heightened bilateral tensions, supporting influence operations, or as a precursor to kinetic escalation.
- RedEcho has strong infrastructure and victimology overlaps with Chinese groups APT41/Barium and Tonto Team, while ShadowPad is used by at least 5 distinct Chinese groups.
- The high concentration of IPs resolving to Indian critical infrastructure entities communicating over several months with a distinct subset of AXIOMATICASYMPTOTE servers used by RedEcho indicate a targeted campaign, with little evidence of wider targeting in Recorded Future's network telemetry.

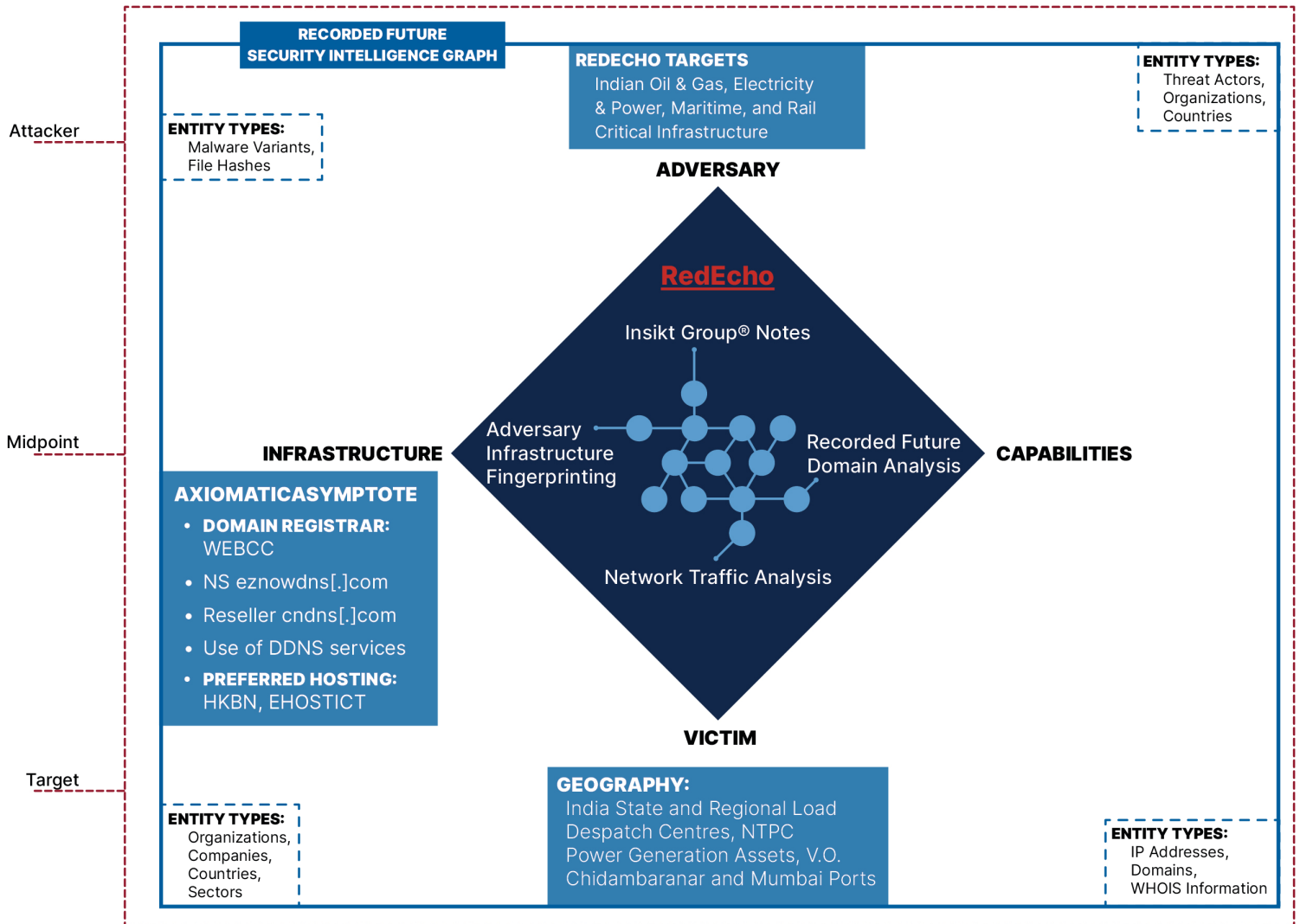


Figure 1: High-level RedEcho TTPs and Recorded Future data sourcing graphic (Source: Recorded Future)

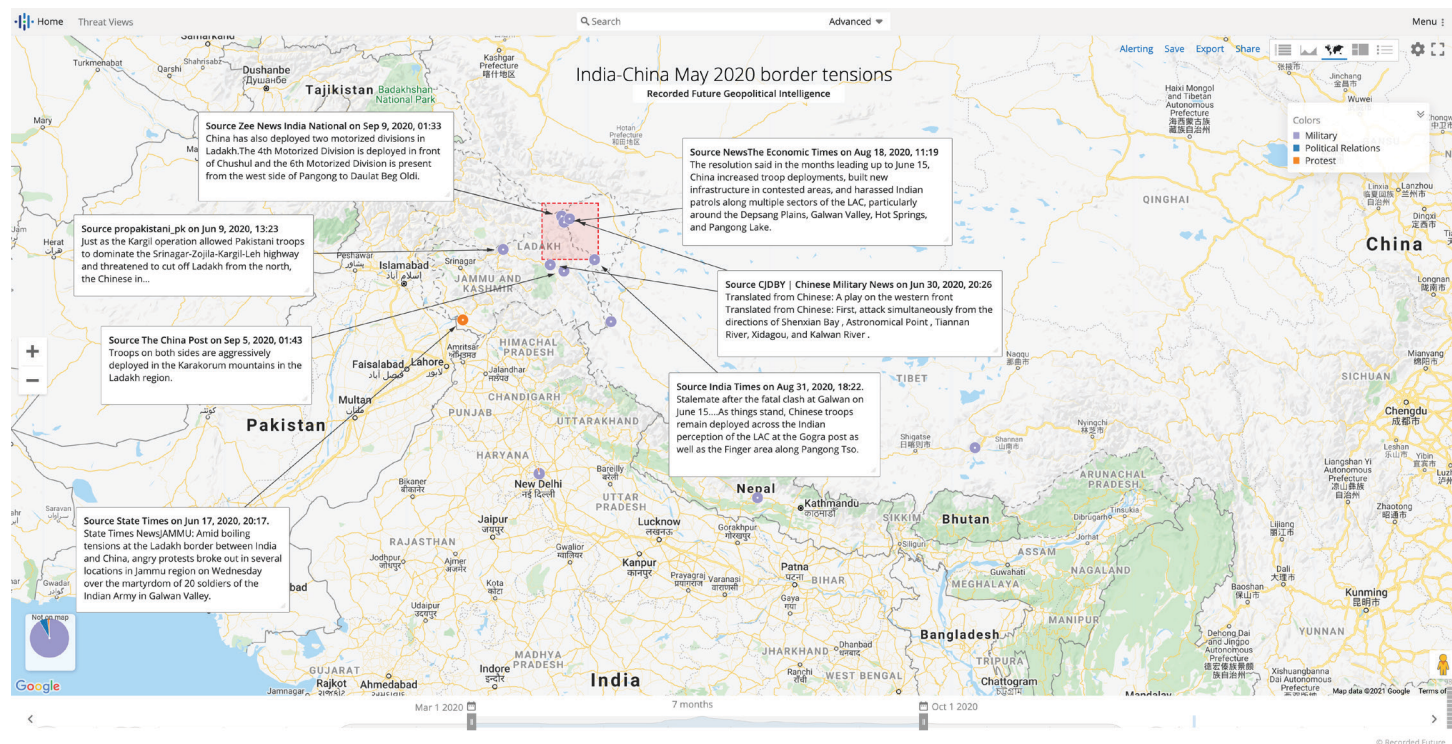


Figure 2: Border skirmishes between Indian and Chinese troops in the Galwan valley in 2020 (Source: Recorded Future Geopolitical Intelligence)

Background

India and China's Escalating Tensions

Recent years have highlighted a growing rivalry between the world's two most populous countries, as India's economy and geopolitical ambitions seek to compete with those of China. Since May 5, 2020, Indian and Chinese troops have [repeatedly skirmished](#) with one another along the India-China border. Reports indicate several likely causes for the escalation, including China's being more assertive in border regions in light of international pressure over the handling of the COVID-19 pandemic, and India's construction of transportation infrastructure in contested areas. China [reportedly](#) amassed a large concentration of troops near the border with India following the initial border escalation, and the dispute appears [unresolved](#). In June 2020, the Indian government announced it was [banning](#) the video-sharing social media platform TikTok from the country, citing fears that the app, whose parent company is the Chinese tech giant ByteDance, might be used to collect data on citizens and potentially also be used for espionage to benefit the Chinese government through a wide-ranging [cybersecurity law](#). By late-November 2020, the Indian government had [subsequently banned over 200 Chinese apps](#) in what was described as a "Digital Strike" in response to the Sino-Indian border clashes by India's technology minister.

These escalating tensions have also been reflected through increased cyber espionage activity by both sides. For example, we observed the suspected Indian state-sponsored group Sidewinder target Chinese military and government entities in 2020, in activity overlapping with recent Trend Micro [research](#). In the lead-up to the May 2020 skirmishes, we observed a noticeable increase in the provisioning of PlugX malware C2 infrastructure, much of which was subsequently used in intrusion activity targeting Indian organizations. The PlugX activity included the targeting of multiple Indian government, public sector, and defense organizations from at least May 2020. Detailed reporting on these suspected intrusions is available to Recorded Future clients. While not unique to Chinese cyber espionage activity, PlugX has been heavily used by China-nexus groups for many years. Throughout the remainder of 2020, we identified a heavy focus on the targeting of Indian government and private sector organizations by multiple Chinese state-sponsored threat activity groups.

Recorded Future Command and Control List, PlugX India, China Protest, Military, Political, Arms and Nuclear, Political Relations

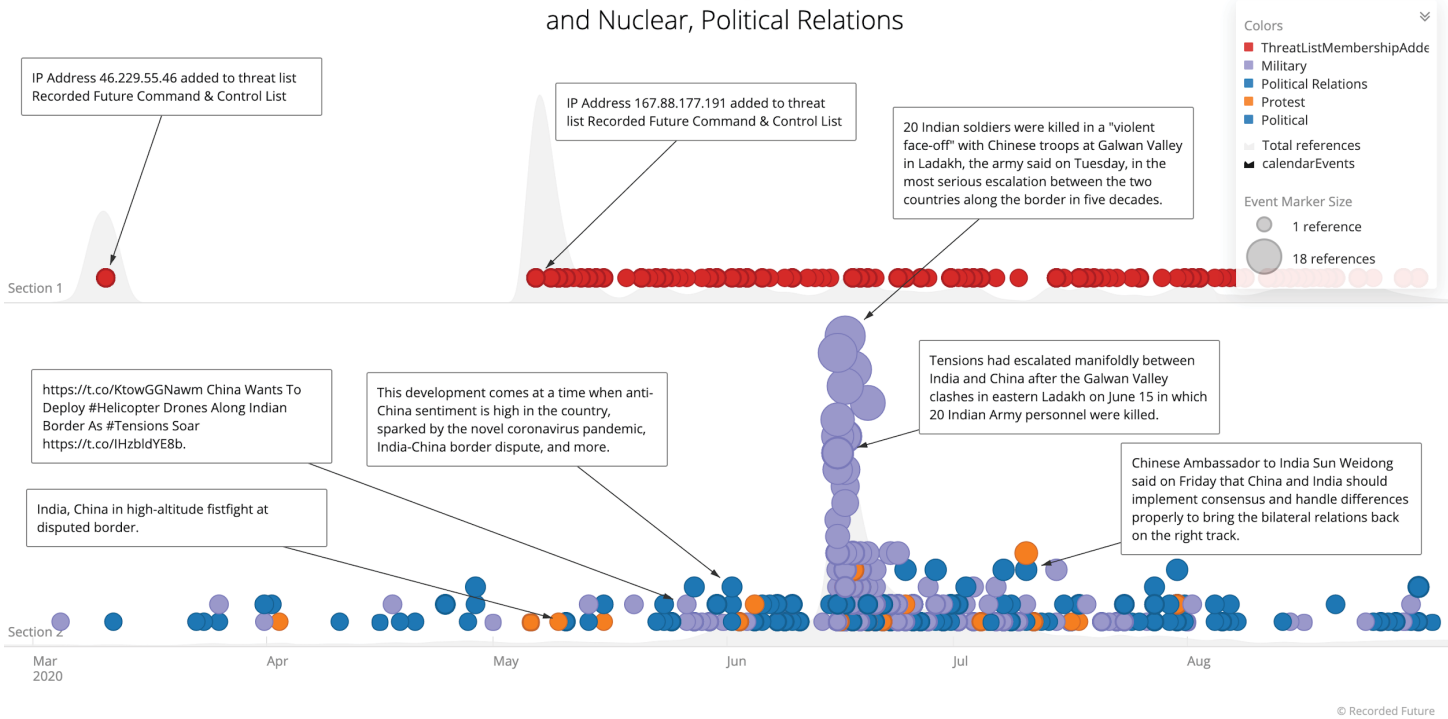


Figure 3: Timeline of Recorded Future PlugX C2 detections aligned with reports of increased geopolitical and military tension between India and China (Source: Recorded Future)

ShadowPad — From Exclusivity to Widespread Use

ShadowPad is a modular backdoor first identified in the Netsarang [compromise](#) in 2017, an intrusion later [attributed](#) to APT41 (BARIUM) by FireEye. While ShadowPad was initially considered exclusive to APT41, additional China-nexus groups began using ShadowPad in network intrusion campaigns from late 2019. We assess that the sharing of ShadowPad is prevalent across groups affiliated with both Chinese Ministry of State Security (MSS) and groups affiliated with the People's Liberation Army (PLA), and is likely linked to the presence of a centralized ShadowPad developer or quartermaster responsible for maintaining and updating the tool.

Presently, we are aware of at least 5 Chinese threat activity groups using ShadowPad, including [APT41](#), [Tonto Team](#), [groups using the Icefog malware](#), [KeyBoy](#), and [Tick](#). Most recently, ShadowPad infrastructure was also [connected to](#) a compromise impacting the Mongolian business management suite Able Software. This intrusion featured tooling overlaps with Chinese-nexus groups TA428 and LuckyMouse, suggesting that the sharing of ShadowPad across Chinese threat activity groups continues to increase.

In September 2020, 5 Chinese APT41 operators were [indicted](#) by the United States (US) government and linked to the front company Chengdu 404 Network Technology. One of the accused previously claimed to be “very close” to the MSS, continuing an [established trend](#) of Chinese private contractors and front companies conducting cyber espionage activity on behalf of the MSS. Conversely, Tonto Team has been [linked](#) to the PLA, specifically the Shenyang Military Region Technical Reconnaissance Bureau. ShadowPad is the latest in a long line of examples of custom capabilities being shared across disparate Chinese threat activity groups for use in cyber espionage activity.

Threat Analysis

The network infrastructure used in ShadowPad infections is tracked by Insikt Group as AXIOMATICASYMPTOTE. This technique fingerprints unique characteristics including header responses and similar network components. Using a combination of proactive infrastructure detections, domain analysis, and network traffic analysis, we have determined that a subset of these AXIOMATICASYMPTOTE servers are being used by a China-linked activity group we track as RedEcho, to target a large swath of India's power sector.

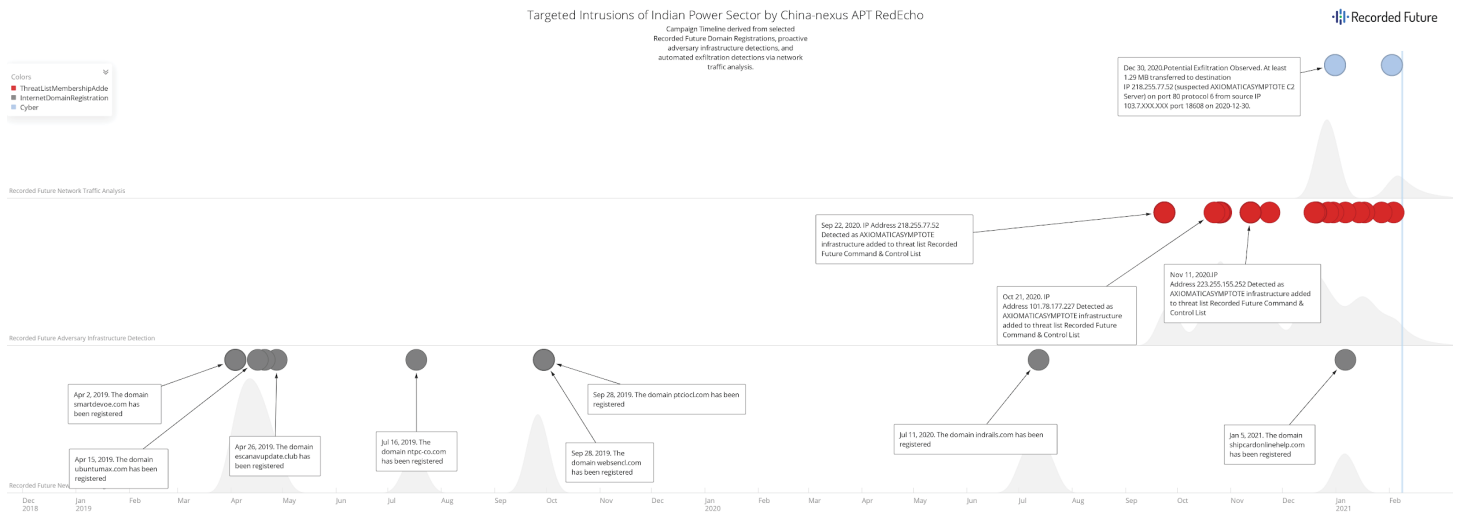


Figure 4: RedEcho campaign timeline highlighting new domain registrations, proactive adversary infrastructure detection, and suspected exfiltration events from targeted networks, derived from Recorded Future Network Traffic Analysis (Source: Recorded Future)

RedEcho Infrastructure TTPs

A subset of the RedEcho AXIOMATICASYMPTOTE servers listed in table 1 below were configured with domains spoofing various Indian power generation and electricity transmission entities. For example, the ntpc-co[.]com domain is likely a typosquat of ntpc[.]co[.]in, the website of Indian power generation company NTPC Limited. The domain was first registered in July 2019, as noted in the Recorded Future new domain registration feed:

Typosquat and brand abuse detection are two of the many features of Recorded Future's Brand Intelligence module, enabling organizations to proactively hunt for suspicious infrastructure as it is being established by adversaries.

FIRST REFERENCE

Domain Registration
 "The domain ntpc-co.com has been registered"
 Source New Domain Registrations on Jul 16, 2019, 09:00 • [Reference Actions](#)

Figure 5: New Domain Registration reference in the Recorded Future portal (Source: Recorded Future)

AXIOMATICASYMPTOTE IP Address	Domain(s)	First Seen	Hosting Provider
101[.]78[.]177[.]227	websencl[.]com ptciocl[.]com	2020-06-12	HKBN Enterprise Solutions HK Limited
101[.]78[.]177[.]252	ptciocl[.]com	2020-12-25	HKBN Enterprise Solutions HK Limited
210[.]92[.]118[.]132	ntpc-co[.]com	2020-12-14	EHOSTICT
218[.]255[.]77[.]52	ptciocl[.]com	2019-09-29	HKBN Enterprise Solutions HK Limited
223[.]255[.]151[.]74	websencl[.]com	2020-11-18	HKBN Enterprise Solutions HK Limited
223[.]255[.]155[.]231	ubuntumax[.]com	2021-01-25	HKBN Enterprise Solutions HK Limited
27[.]255[.]92[.]83	ubuntumax[.]com	2021-02-06	EHOSTICT
223[.]255[.]155[.]238	www.shipcardonlinehelp[.]com	2020-10-12	HKBN Enterprise Solutions HK Limited
27[.]255[.]94[.]29	ntpc-co[.]com	2020-08-20	EHOSTICT
218[.]255[.]77[.]54	www.smartdevoe[.]com	2020-02-05	HKBN Enterprise Solutions HK Limited
223[.]255[.]151[.]85	www.smartdevoe[.]com	2020-12-19	HKBN Enterprise Solutions HK Limited
101[.]78[.]177[.]242	www.smartdevoe[.]com	2020-07-21	HKBN Enterprise Solutions HK Limited
218[.]255[.]77[.]40	ptciocl[.]com	2020-11-24	HKBN Enterprise Solutions HK Limited

Table 1: List of initially identified RedEcho AXIOMATICASYMPTOTE infrastructure cluster used in targeting of Indian power sector

Insikt Group profiled the identified RedEcho operational infrastructure and identified a pattern of behavior, in line with the concept of viewing network indicators as [composite objects](#). RedEcho's operational infrastructure modus operandi in the identified intrusion campaign can be summarized as follows:

- Domains were registered through the registrar WEBCC and used an uncommon authoritative name server, eznwdns[.]com
- RedEcho operational infrastructure associated with the Chinese domain and infrastructure reseller cndns[.]com
- Used the WhoisProtection WHOIS privacy protection service
- AXIOMATICASYMPTOTE infrastructure hosted on HKBN Enterprise Solutions HK Limited (AS9381) and EHOSTICT (AS45382)
- Domains spoofed (lexically similar) Indian entities or featured strings referencing India
- Used a common top level domain (.com)
- Used dynamic DNS domains for operational infrastructure (further details below)

While none of these characteristics are individually unique to RedEcho, viewing these holistically identified unique behaviors in combination is likely indicative of RedEcho activity. Based on these highlighted TTPs, we identified additional domains that were likely related, which featured overlaps with known AXIOMATICASYMPTOTE servers as well as historical hosting data for domains within the highlighted infrastructure cluster.

Further pivots constrained to shared historic hosting infrastructure identified a further cluster of RedEcho dynamic DNS (DDNS) domains which share the same Indian-themed domain naming pattern and links to AXIOMATICASYMPTOTE servers:

RedEcho Victimology

Derived from Recorded Future Network Traffic Analysis, we were able to determine a clear and consistent pattern of Indian organizations being targeted in this campaign through the behavioral profiling of network traffic to adversary infrastructure. Much of the observed network activity inbound to the AXIOMATICASYMPTOTE infrastructure was over SSL via TCP port 443. We also noted substantial inbound traffic to the AXIOMATICASYMPTOTE infrastructure indicative of HTTP proxying activity over TCP 8080 and DNS requests (UDP 53) for the C2 domains hosted on AXIOMATICASYMPTOTE servers (see below Infrastructure section).

Domain	IP Address	Comment
indiasung[.]com	223[.]255[.]155[.]243 180[.]150[.]226[.]216	180[.]150[.]226[.]216 — Confirmed AXIOMATICASYMPTOTE server.
ixrails[.]com	223[.]255[.]155[.]243 101[.]78[.]177[.]227	101[.]78[.]177[.]227 — Confirmed AXIOMATICASYMPTOTE server.
pandorarve[.]com	223[.]255[.]155[.]247 223[.]255[.]155[.]252	223[.]255[.]155[.]252 — Confirmed AXIOMATICASYMPTOTE server.
indrails[.]com	223[.]255[.]155[.]237	Matches infrastructure TTPs and Indian railway-themed.
escanavupdate[.]club	218[.]255[.]77[.]160	Multiple hosting overlaps within the infrastructure cluster. Likely spoofing Indian antivirus provider eScan AV.
astudycarsceu[.]net	27[.]255[.]194[.]21	Confirmed AXIOMATICASYMPTOTE server, matches infrastructure TTPs, and overlapping victimology.

Table 2: Additional likely RedEcho domains matching infrastructure TTPs

Domain	AXIOMATICASYMPTOTE IP Address
railway.sytes[.]net	223[.]255[.]155[.]235
modibest.sytes[.]net	223[.]255[.]155[.]235
indrra.ddns[.]net	218[.]103[.]197[.]112
indianrailway.hopto[.]org	223[.]255[.]155[.]235
inraja.ddns[.]net	218[.]103[.]197[.]112
railways.hopto[.]org	223[.]255[.]155[.]235

Table 3: RedEcho dynamic DNS domains

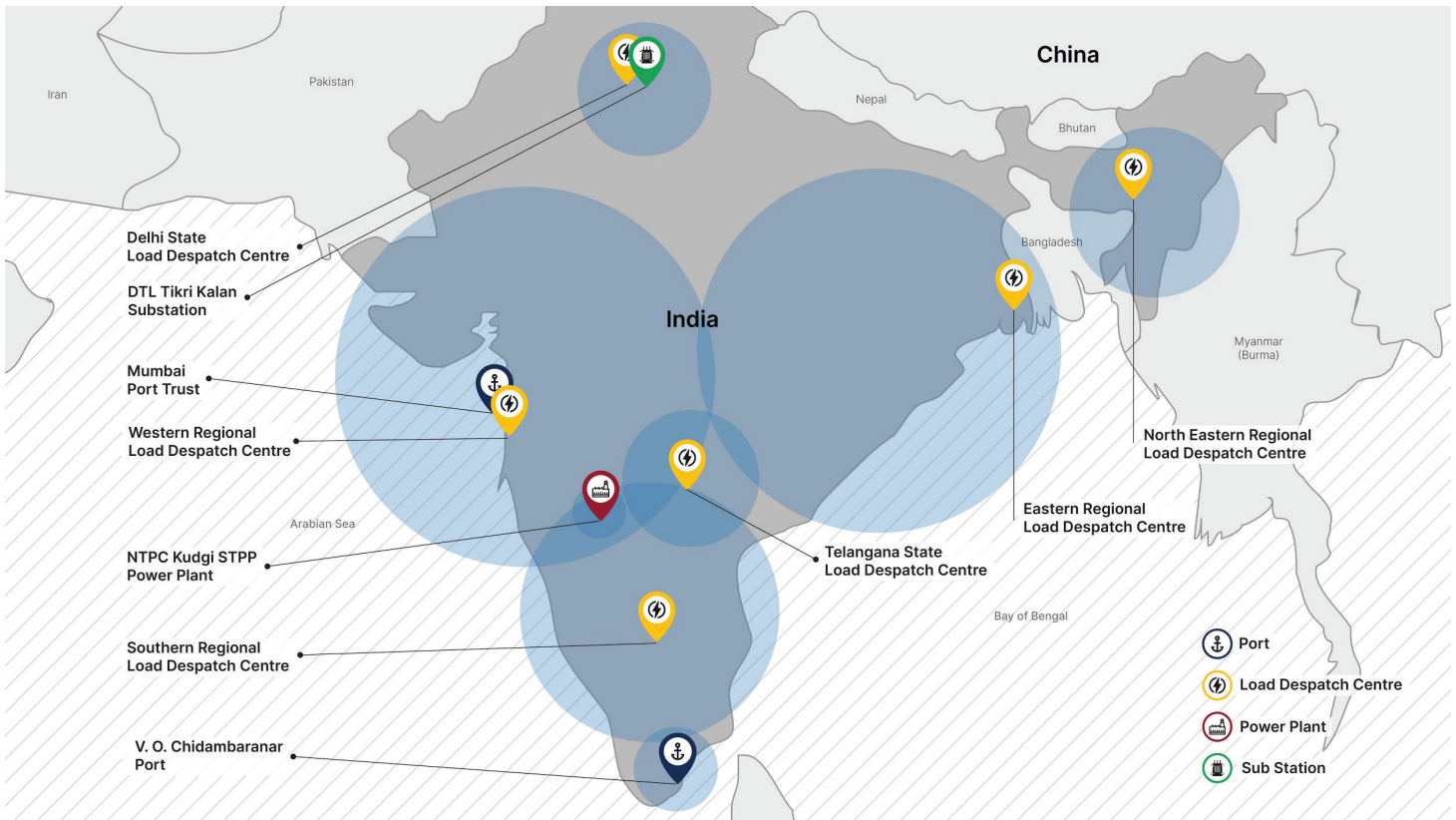


Figure 6: Suspected Indian power sector victims of RedEcho targeted intrusions (Source: Recorded Future, Map data ©2021 Google)

In total, we identified 21 IP addresses resolving to 10 distinct Indian organizations in the power generation and transmission sector that were targeted, with a further 2 organizations in the maritime sector. All 12 organizations likely qualify as critical infrastructure, per the Indian National Critical Information Infrastructure Protection Centre (NCIIPC) definition.

Within India’s power sector, RedEcho conducted suspected network intrusions targeting at least 4 out of the country’s 5 Regional Load Despatch Centres (RLDCs), alongside 2 State Load Despatch Centres (SLDCs). RLDCs and SLDCs are

responsible for ensuring real-time integrated operation of India’s power grid through balancing electricity supply and demand to maintain a stable grid frequency. Additionally, local media reporting previously linked an October 2020 power outage in Mumbai to the identification of malware at a Padgha-based State Load Despatch Centre. At this time, the alleged link between the outage and the discovery of the unspecified malware variant remains unsubstantiated. However, this disclosure provides additional evidence suggesting the coordinated targeting of Indian Load Despatch Centres.

Suspected Victim Organization	Description
Power System Operation Corporation Limited	Government of India-owned enterprise under Ministry of Power
NTPC Limited	Indian energy conglomerate concerned with electricity generation and allied activities
NTPC Kudgi STPP	Power Plant
Western Regional Load Despatch Centre	RLDC
Southern Regional Load Despatch Centre	RLDC
North Eastern Regional Load Despatch Centre	RLDC
Eastern Regional Load Despatch Centre	RLDC
Telangana State Load Despatch Centre	SLDC
Delhi State Load Despatch Centre	SLDC
DTL Tikri Kalan (Mundka), Delhi Transco Ltd	Substation
V. O. Chidambaranar Port	Maritime port
Mumbai Port Trust	Maritime port

Table 4: List of suspected victims of RedEcho campaign targeting Indian critical infrastructure in 2020

Other RedEcho intrusions within the Indian power sector included the targeting of a high-voltage transmission substation and a coal-fired thermal power plant. The targeting of these critical power assets offer limited economic espionage opportunities, but pose significant concerns over potential pre-positioning of network access to support other Chinese strategic objectives.

Finally, two Indian seaports were also targeted by RedEcho. The high concentration of IPs resolving to Indian critical infrastructure entities that were identified communicating with a distinct subset of AXIOMATICASYMPTOTE servers, indicate a targeted campaign with little evidence of wider targeting in Recorded Future’s network telemetry.

RedEcho Attribution

At least 3 of the targeted Indian IP addresses were previously seen in a suspected APT41/Barium-linked campaign targeting the Indian Oil and Gas sectors in November.2020

An even larger proportion of the RedEcho-targeted Indian IP addresses were observed communicating with 2 AXIOMATICASYMPTOTE servers hosting a large number of DDNS domains (91.204.224[.]14 and 91.204.225[.]216). This included overlaps with APT41/Barium activity previously reported by [Microsoft](#), such as the domain bguha.serveuser[.]com.

Historical hosting overlaps also exist between RedEcho DDNS domain railway.sytes[.]net and the previously reported APT41/Barium cluster. However, it is important to note that several DDNS domains attributed to Barium by Microsoft were also previously linked to Tonto Team threat activity in public reporting from [Trend Micro](#). In their report, Trend Micro also noted that Tonto Team targeted India’s Oil and Gas and Energy industries.

Despite some overlaps with previously detected APT41/Barium-linked activity and possible further overlaps with Tonto Team activity, we currently do not believe there is enough evidence to firmly attribute the activity in this particular Indian power sector targeting to either group and therefore continue to track it as a closely related, but distinct, activity group, RedEcho.



Figure 7: Location of suspected victim NTPC Kudgi STPP (Source: Imagery ©2021 CNES/Airbus, Maxar Technologies, Map data ©Google)

A Note on Tradecraft

Recorded Future's [Security Intelligence Graph](#) continues to evolve by distilling vast swaths of open source, dark web, and technical data and combining it with the intimate knowledge of attacker tradecraft from analysts. Pioneered within Insikt Group and Data Science and forming a core piece of this research has been the development of new Network Traffic Analysis analytics that enable users to discover and track suspected targeted intrusion activity derived from validated technical data sources.

As documented recently in our [2020 Adversary Infrastructure Report](#), we proactively detect malicious infrastructure using a combination of passive and active scanning approaches. In 2020, over 10,000 unique servers used by malicious threat actors were identified in this manner. We apply a series of filters and algorithms to spot suspicious network traffic concerning these detected malicious servers, highlighting possible targeted intrusion activity. Intelligence Card extensions within the Recorded Future Platform then allow users to enrich this information further using data from close partners such as SecurityTrails, thereby enabling Recorded Future Threat Intelligence or SecOps [module](#) users to efficiently map out prospective adversary campaigns.

Mitigations

We recommend that users conduct the following measures to detect and mitigate activity associated with RedEcho activity:

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains listed in the appendix.
- Recorded Future proactively detects and logs malicious server configurations in the Command and Control Security Control Feed. The Command and Control list includes tools used by RedEcho and Chinese state-sponsored threat activity groups, such as AXIOMATICASYMPTOTE. Recorded Future clients should alert on and block these C2 servers to allow for detection and remediation of active intrusions.
- Multiple state-sponsored and financially motivated threat activity groups continue to use DDNS domains in network intrusion activity. All TCP/UDP network traffic involving DDNS subdomains should be blocked and logged (using [DNS RPZ](#) or similar).
- All domains using eznowdns[.]com as an authoritative nameserver should be blocked and logged (using [DNS RPZ](#) or similar).
- Recorded Future Threat Intelligence, Third-Party Intelligence, and SecOps Intelligence [module](#) users can monitor real-time output from Network Traffic Analysis analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.
- Monitor for domain abuse, such as typosquat domains spoofing your organization, through the Recorded Future Brand Intelligence [module](#).

Analysis Report

Network Traffic Analysis for [REDACTED]

IP Addresses: [REDACTED]
210.92.18.132

Network Ports: 17035
80

Network Protocol: 6

Malware: AXIOMATICASYMPTOTE

MITRE ATT&CK Identifier: T1041 (Exfiltration Over C2 Channel)

Source Network Traffic Analysis on Feb 2, 2021, 13:16 • Document Actions

1. MITRE ATT&CK Identifier: T1041
2. Transfer Volume: 4.12 MB
3. Victim IP: [REDACTED]
4. Victim Port: 17035
5. Command & Control IP: 210.92.18.132
6. Command & Control Port: 80
7. Protocol: 6
8. Malware: AXIOMATICASYMPTOTE
9. Potential Command & Control Domain(s): ntpc-co.com
- 10.

Recorded Future

IP ADDRESS

210.92.18.132

ASN	AS45382
ORG	EHOSTICT
GEO	South Korea
References	2
First Reference	Dec 29, 2020
Latest Reference	Dec 29, 2020

95
VERY MALICIOUS RISK SCORE
2 of 53 Risk Rules Triggered

TRIGGERED RISK RULES

- Current C&C Server - 1 sighting on 1 source
Recorded Future Command & Control List: Command & Control host identified on Dec 29, 2020.
- Actively Communicating C&C Server - 1 sighting on 1 source
Recorded Future Network Traffic Analysis: Identified as C&C server for 1 malware family: Axiomaticasymptote. Communication observed on TCP:8080, TCP:443, TCP:80. Last observed on Jun 27, 2021.

Recorded Future

DOMAIN

ntpc-co.com

Notes: 1 Insikt Group Note

References: 5

First Reference: Jul 16, 2019

Latest Reference: Feb 2, 2021

65
MALICIOUS RISK SCORE
1 of 46 Risk Rules Triggered

TRIGGERED RISK RULES

Recently Reported by Insikt Group - 1 sighting on 1 source
Insikt Group: 1 report: Indian Energy and Defense Companies Likely Targeted by China-nexus Group Using ShadowPad and PlugX. Most recent link (Dec 30, 2020): https://app.recordedfuture.com/live/sc/2JdaWII3aTQ.

ADDITIONAL DOMAIN INFORMATION

DNS Records

IP Address: A 210.92.18.132 ● 95

No Mail Server

Name Server

- NS ns4.eznwdns.com ● 5
- NS ns5.eznwdns.com ● 5
- NS ns6.eznwdns.com ● 5
- NS ns3.eznwdns.com ● 5
- NS ns2.eznwdns.com ● 5
- NS ns1.eznwdns.com ● 5

IP History powered by SecurityTrails

IP: 210.92.18.132

Total # Domains: 2 domain(s) in the last 120 days

History

- ntpc-co.com Risk: 65
DNS Name: ntpc-co.com
A Records
Resolution Period: 2021-01-05 to now (Last Resolved: 2021-02-01)
Resolution Period: 2020-12-14 to 2021-01-01
- www.ntpc-co.com Risk: 0

More Info SecurityTrails

Figure 8: Pivoting between technical data sets within the Recorded Future portal (Source: Recorded Future)

Outlook

In this research, we outlined a series of suspected targeted intrusions against India's power sector that were observed beginning in mid-2020. The intrusions were conducted by a China-linked activity group we track as RedEcho. The group made heavy use of AXIOMATICASYMPTOTE — a term we use to track infrastructure that comprises ShadowPad C2s, which is shared between several Chinese threat activity groups, including APT41/Barium, Tonto team, the Icefog cluster, KeyBoy, and Tick.

The intrusions overlap with previous Indian energy sector targeting by Chinese threat activity groups in 2020 that also used AXIOMATICASYMPTOTE infrastructure. Therefore, the focus in targeting India's electricity system possibly indicates a sustained strategic intent to access India's energy infrastructure. Network access to Regional Load Despatch Centres provide minimal benefit for economic espionage objectives, but are of strategic interest to enable access pre-positioning for a variety of potential outcomes such as:

- To send a robust signaling message as a “show of force”
- To enable influence operations to sway public opinion during a diplomatic confrontation
- To support potential future disruptive cyber operations against critical infrastructure

As bilateral tensions continue to rise, we expect to see a continued increase in cyber operations being conducted by China-linked groups such as RedEcho in line with national strategic interests. While economic recovery from the impact of the coronavirus pandemic will be a priority for both countries, the increasing rhetoric and the kinetic escalation of border tensions suggests there is clearly mistrust and uncertainty within each government. Further, China will likely also continue to exert influence over other nations, particularly those that are within the sphere of influence of their BRI investment program, which may lead to more cyber operations aimed at furthering strategic advantage.

Appendix — Indicators

Readers can access the indicators listed below in our public Insikt Group Github repository: <https://github.com/Insikt-Group/Research> (RedEcho - February 2021).

```
ntpc-co[.]com
websencl[.]com
ptciocl[.]com
ubuntumax[.]com
www.shipcardonlinehelp[.]com
www.smartdevoe[.]com
www.astudycarsceu[.]net
www[.]indiasunsung[.]com
ixrails[.]com
pandorarve[.]com
indrails[.]com
escanavupdate[.]club
railway.sytes[.]net
modibest.sytes[.]net
indrira.ddns[.]net
indianrailway.hopto[.]org
inraja.ddns[.]net
railways.hopto[.]org
101[.]78[.]177[.]227
101[.]78[.]177[.]252
210[.]92[.]18[.]132
218[.]255[.]77[.]52
223[.]255[.]151[.]74
223[.]255[.]155[.]231
223[.]255[.]155[.]235
223[.]255[.]155[.]238
27[.]255[.]94[.]29
27[.]255[.]94[.]21
27[.]255[.]92[.]83
223[.]255[.]151[.]85
101[.]78[.]177[.]242
218[.]255[.]77[.]40
218[.]255[.]77[.]54
223[.]255[.]155[.]243
180[.]150[.]226[.]216
223[.]255[.]155[.]247
223[.]255[.]155[.]252
223[.]255[.]155[.]237
218[.]255[.]77[.]60
```

Recorded Future Threat Activity Group and Malware Taxonomy

Recorded Future's research group, Insikt, tracks threat actors and their activity, focusing on state actors from China, Iran, Russia, and North Korea, as well as cyber criminals - individuals and groups - from Russia, CIS states, China, Iran, and Brazil. We emphasize tracking activity groups and where possible, attributing them to nation state government, organizations, or affiliate institutions.

Our coverage includes:

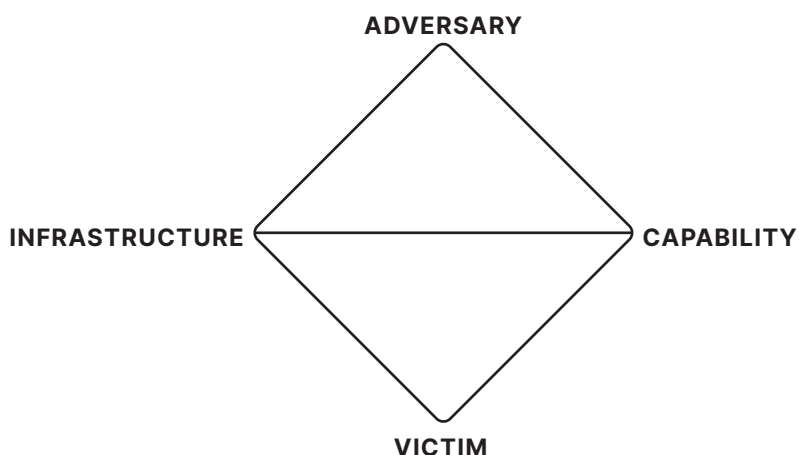
- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors.
- Recorded Future-identified, suspected nation state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other industry established groups.
- Cybercriminal individuals and groups established and named by Recorded Future
- Newly emerging malware, as well as prolific, persistent commodity malware

Insikt Group names a new threat activity group or campaign when analysts have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence, derived from our Security Intelligence Graph. We can tie this to a threat actor only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely-utilized or recognized name for a particular group when the public body of empirical evidence is clear the activity corresponds to a known group.

Insikt Group utilizes a simple color and phonetic alphabet naming convention for new nation state threat actor groups or campaigns. The color corresponds to that nation's flag colors, currently represented below, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.

For newly identified cybercriminal groups, Insikt Group uses a naming convention corresponding to the Greek alphabet. Where we have identified a criminal entity connected to a particular country, we will use the appropriate country color, and where that group may be tied to a specific government organization, tie it to that entity specifically.

Insikt Group uses mathematical terms when naming newly identified malware.



CHINA



IRAN



NORTH KOREA



RUSSIA

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.