THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

April 6, 2022

Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group

This report details a campaign conducted by a likely Chinese state-sponsored threat activity group 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, PolySwarm, Team Cymru's Pure Signal™, 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 cyber activity. Recorded Future notified the appropriate Indian government departments prior to publication of the suspected intrusions to support incident response and remediation investigations within affected organizations. With thanks to our colleagues at Dragos for early sharing and collaboration.

Executive Summary

In February 2021, Recorded Future's Insikt Group reported on intrusion activity targeting operational assets within India's power grid that we attributed to a likely Chinese state-sponsored threat activity group we track as RedEcho. Following a short lull after the publication of our RedEcho reporting, we have detected ongoing targeting of Indian power grid organizations by China-linked adversaries, frequently using the privately shared modular backdoor ShadowPad. ShadowPad continues to be employed by an ever-increasing number of People's Liberation Army (PLA) and Ministry of State Security (MSS)-linked groups, with its origins linked to known MSS contractors first using the tool in their own operations and later likely acting as a digital quartermaster.

In recent months, we observed likely network intrusions targeting at least 7 Indian State Load Despatch Centres (SLDCs) responsible for carrying out real-time operations for grid control and electricity dispatch within these respective states. Notably, this targeting has been geographically concentrated, with the identified SLDCs located in North India, in proximity to the disputed India-China border in Ladakh. One of these SLDCs was also targeted in previous RedEcho activity. This latest set of intrusions, however, is composed of an almost entirely different set of victim organizations. In addition to the targeting of power grid assets, we also identified the compromise of a national emergency response system and the Indian subsidiary of a multinational logistics company by the same threat activity group. To achieve this, the group likely compromised and co-opted internet-facing DVR/IP camera devices for command and control (C2) of Shadowpad malware infections, as well as use of the open source tool FastReverseProxy (FRP).

Despite a partial troop disengagement between India and China from February 2021, the prolonged targeting of Indian critical infrastructure continues to raise concerns over pre-positioning activity being conducted by Chinese adversaries. While this latest activity displays targeting and capability consistencies with previously identified RedEcho activity, there are also some notable distinctions. At this time, we have not identified technical evidence allowing us to attribute it to RedEcho, and we are currently clustering this latest activity under the temporary group name Threat Activity Group 38 (TAG-38)[1].

Key Judgments

- Given the continued targeting of State and Regional Load Despatch Centres in India over the past 18 months, first from RedEcho and now in this latest TAG-38 activity, this targeting is likely a long-term strategic priority for select Chinese state-sponsored threat actors active within India.
- The prolonged targeting of Indian power grid assets by Chinese state-linked groups offers limited economic espionage or traditional intelligence-gathering opportunities. We believe this targeting is instead likely intended to enable information gathering surrounding critical infrastructure systems or is pre-positioning for future activity.
- The objective for intrusions may include gaining an increased understanding into these complex systems in order to facilitate capability development for future use or gaining sufficient access across the system in preparation for future contingency operations.

1 Typically, Insikt Group publicly names a new threat activity group or campaign, such as RedFoxtrot, when analysts have data corresponding to at least 3 points on the Diamond Model of Intrusion Analysis with at least medium confidence. We will occasionally report on significant activity using a temporary activity clustering name such as TAG-38, where the activity is new and significant but doesn't map to existing groupings and hasn't yet graduated or merged into an established activity group.

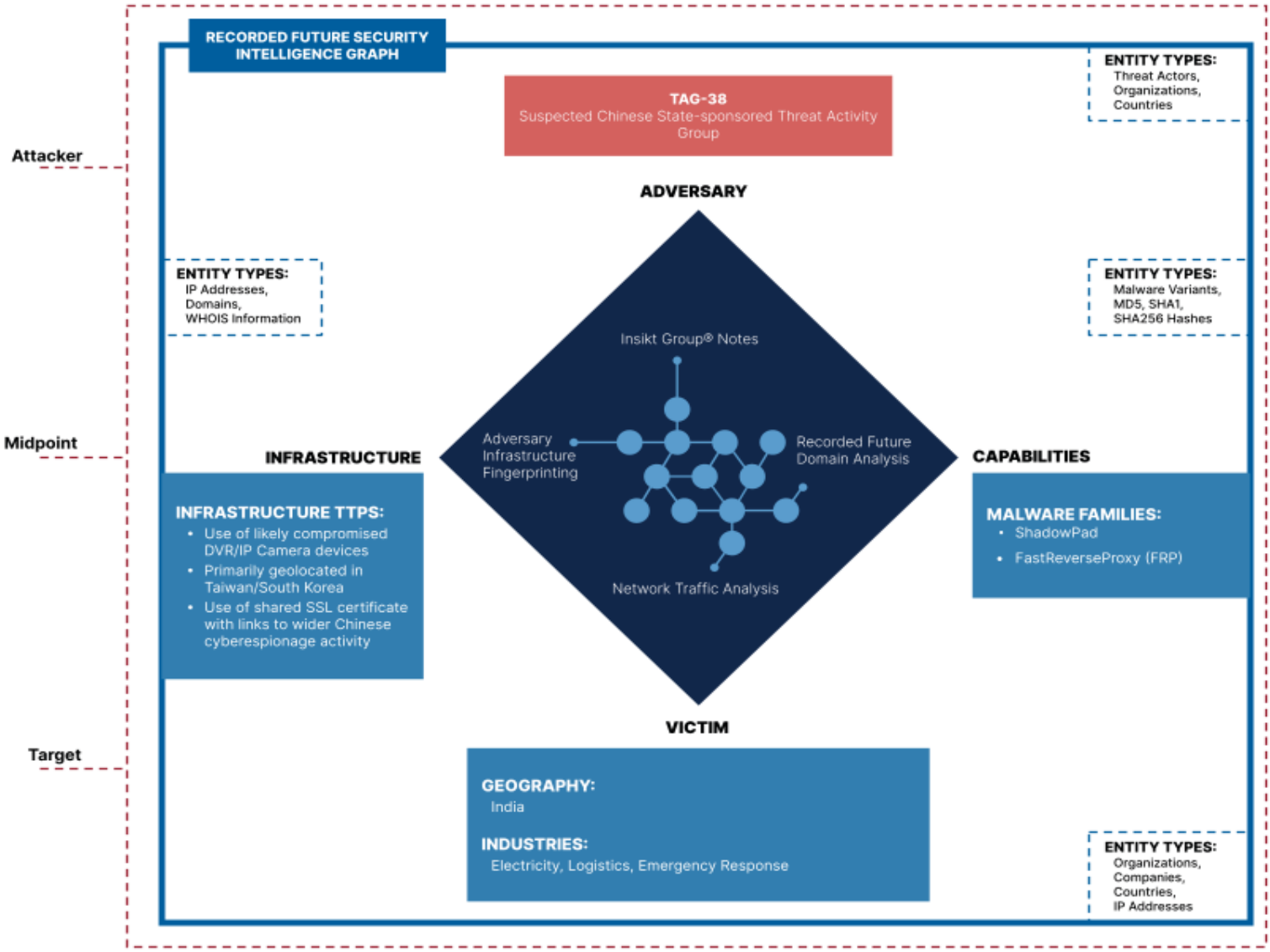

Figure 1: High-level TAG-38 TTPs and Recorded Future data sourcing graphic (Source: Recorded Future)

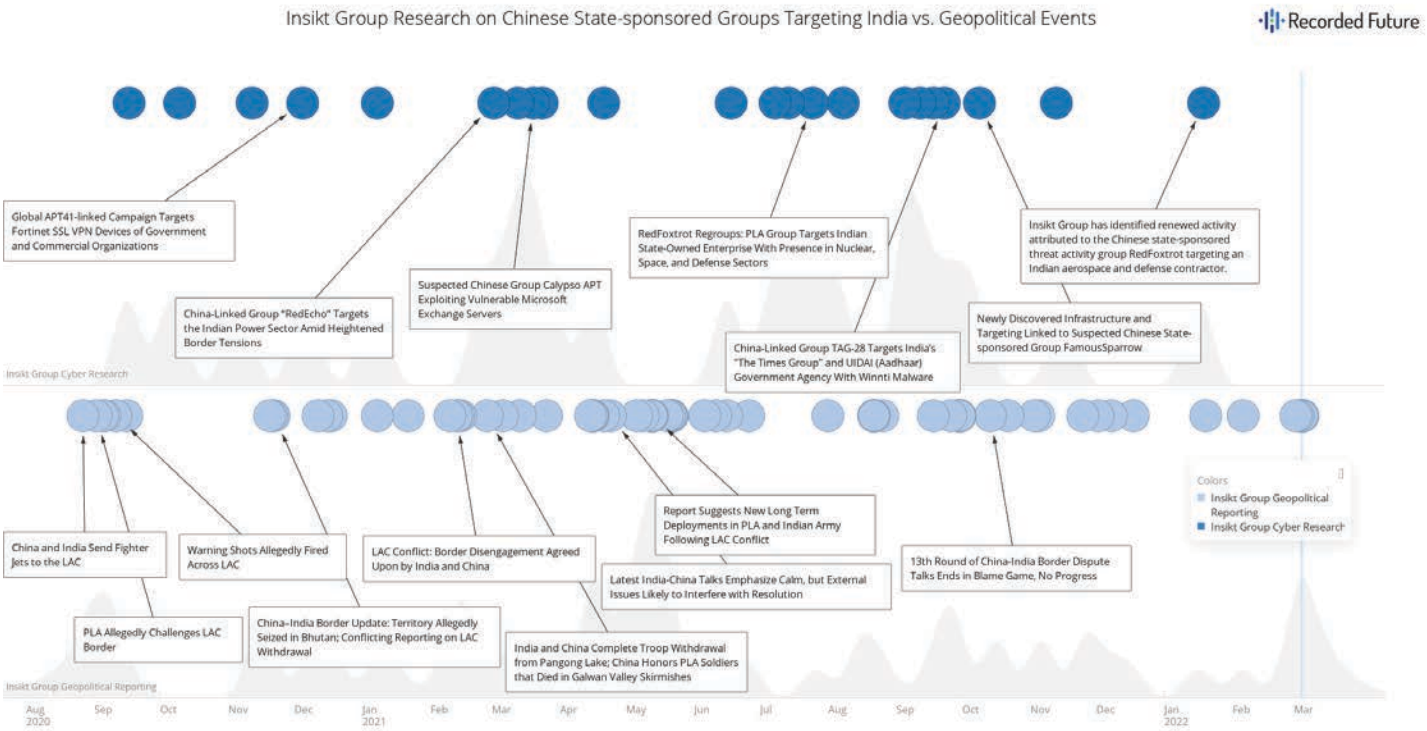

Figure 2: Timeline of Insikt research on Chinese state-sponsored groups targeting India versus geopolitical events (Source: Recorded Future)

Background

India continues to be a major target of Chinese cyber espionage activity, as detailed in historical Recorded Future reporting on RedDelta, RedEcho, RedFoxtrot, TAG-28, and additional client-facing research. Although tensions reduced, aided by partial troop disengagement, in February 2021 following prolonged border stand-offs in the Ladakh region, there has been limited progress between the states regarding respective territorial claims.

Our February 2021 RedEcho report highlighted the compromise of 10 distinct Indian power sector organizations, including 4 of the 5 of the country's Regional Load Despatch Centres (RLDC), 2 ports, a large generation operator, and other operational assets. These assets offer minimal value as economic espionage or other traditional intelligence targets, which led us to assess a likely goal of pre-positioning network access to support Chinese strategic objectives. Following that February 2021 report, we observed the group abandon the operational infrastructure highlighted and shift its infrastructure modus operandi. Despite this, evidence of targeting of Indian power assets and organizations with links to critical infrastructure from Chinese state-sponsored actors continued. This included the targeting of an Indian managed service provider (MSP) and operational technology (OT) vendor using ShadowPad, which aligns with activity described in recent Dragos reporting. We attribute this particular activity to a separate activity group we track as Threat Activity Group 26 (TAG-26). We have observed TAG-26 targeting multiple high-value organizations in India using ShadowPad, Poison Ivy, and the RoyalRoad RTF weaponizer.

The use of ShadowPad across Chinese activity groups continues to grow over time, with new clusters of activity regularly identified using the backdoor as well as continued adoption by previously tracked clusters. At this time, we track at least 10 distinct activity groups with access to ShadowPad, which is assessed to have likely been originally developed and used by MSS-linked contractors linked to the APT41 (BARIUM) intrusion set.

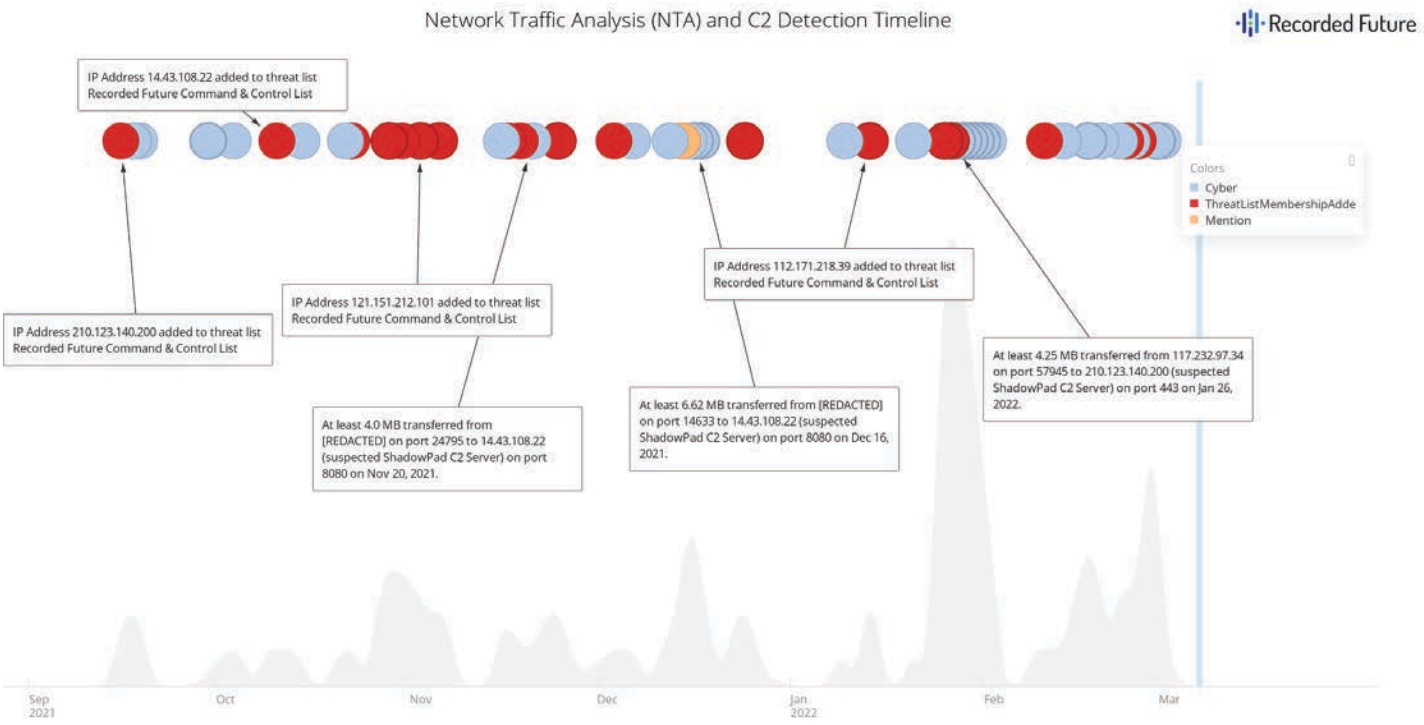

Figure 3: Timeline of TAG-38 C2 infrastructure detection and network traffic analysis (NTA) exfiltration events (Source: Recorded Future)

Threat Analysis

Since at least September 2021, we have observed TAG-38 intrusions targeting the identified victim organizations. The group has employed probable compromised infrastructure for command and control of ShadowPad implants used to target the identified networks, as well as using the open source tool Fast Reverse Proxy (FRP). Figure 3 highlights ongoing TAG-38 C2 detection and network traffic analysis exfiltration events from victim networks within the Recorded Future platform between September 2021 and March 2022.

Targeting of Indian Power Sector

The identified victimology within this latest campaign is confined to Indian targets, specifically at least 7 SLDCs, the Indian subsidiary of a multinational logistics company, and a national emergency response system. As shown in Figure 4, the identified SLDCs were all located in Northern India, in proximity to the disputed China-India border in Ladakh. SLDCs are responsible for carrying out real-time operations for grid control and electricity dispatch within these respective states, similar to the Regional Load Despatch Centres (RLDCs) previously targeted in reported RedEcho activity. This makes these organizations critical for maintaining grid frequency and stability, with SLDCs maintaining access to supervisory control and data acquisition (SCADA) systems present across respective states for the purpose of grid control and electricity dispatch. At this time, we have not observed evidence of access to industrial control system (ICS) environments in this activity.

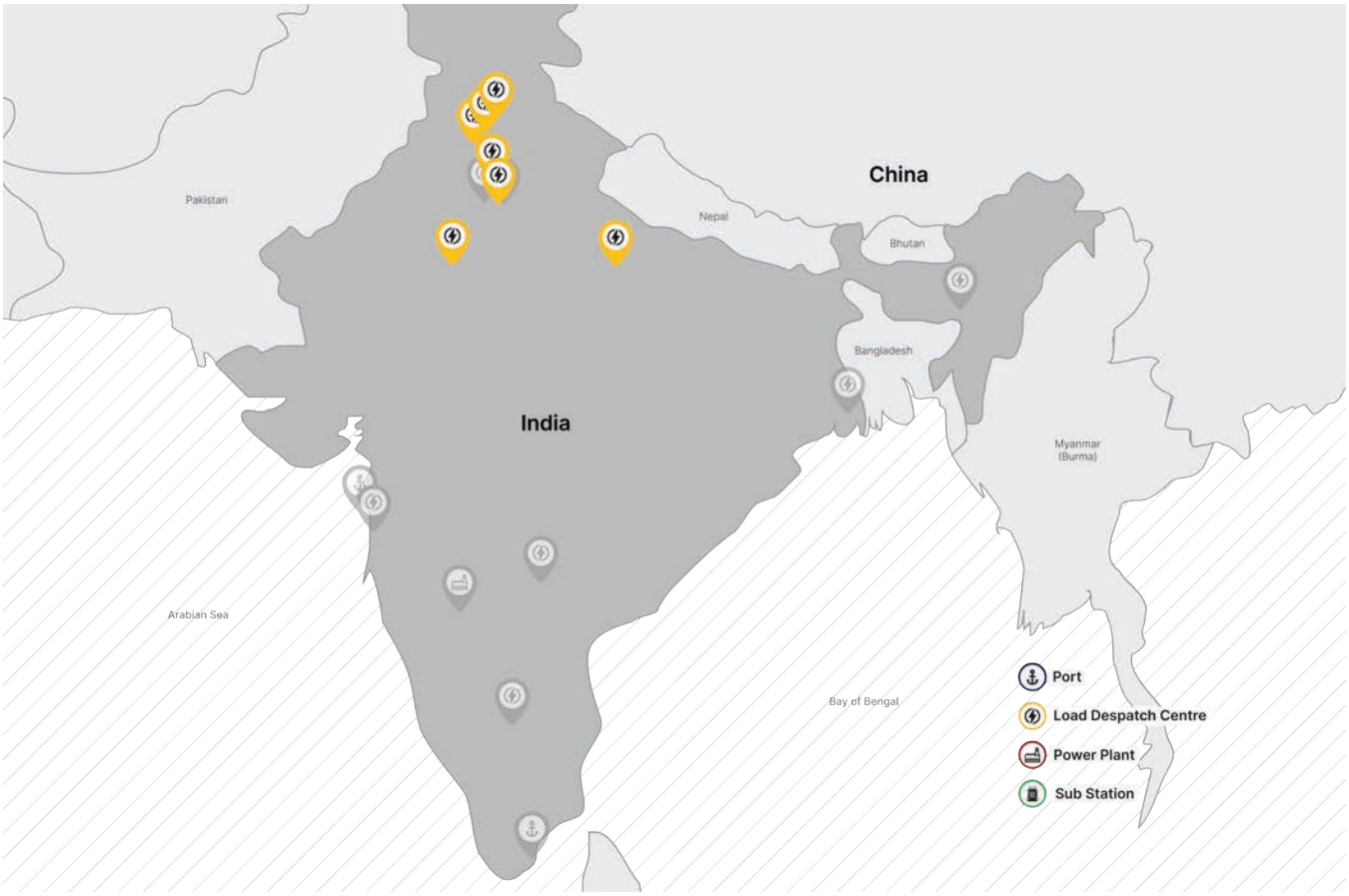

Figure 4: Map of TAG-38 victim State Load Despatch Centre (SLDC) locations. Previously reported RedEcho victim locations also displayed in gray (Source: Recorded Future)

TAG-38 Infrastructure Clustering

Using a combination of proactive infrastructure detection techniques and network traffic analysis, we uncovered a cluster of C2 infrastructure engaged in this prolonged targeting of Indian critical infrastructure over several months. Based on our analysis, the adversary infrastructure cluster identified consists entirely of likely compromised internet-facing, third-party DVR/IP camera devices. The compromise of often poorly secured internet-of-things (IOT) devices such as IP cameras for use in follow-on intrusion activity has previously been seen for threats ranging from Mirai-based botnets (1,2) to the Chinese state-sponsored threat activity group RedBravo (APT31/ZIRCONIUM). At this time, we have not determined the means in which these devices were originally compromised, which may include the use of default credentials. Using a series of analytical techniques and heuristics, we were able to cluster a network of these C2 IPs together, all of which matched all or most of the following criteria:

- Victim infrastructure observed communicating to all of the identified C2 servers consisted solely of the same overlapping Indian power grid victims, logistics company, and Indian emergency response system.
- All C2 servers were likely compromised DVR/IP camera devices and were primarily geolocated in Taiwan or South Korea.
- Likely compromised devices were observed with the default open ports 80/554/9090 associated with the compromised device, as well as an additional actor-controlled port(s) opened for malware C2 communications.
- A large proportion were confirmed as ShadowPad C2 servers using Recorded Future C2 detection methodologies, a technique previously used in historical Insikt Group reporting on RedEcho and other Chinese state-sponsored activity groups (1,2,3).
- A large proportion of the identified C2s had the open source tool Fast Reverse Proxy (FRP) server component configured on port 8443. FRP can read predefined configurations and allows you to expose local services that are hidden behind the NAT or a firewall to the internet. This tool has been abused by numerous state-sponsored groups, including the Iran-linked group Phosphorus and several Chinese actors (1,2).
- A large proportion of the identified C2s shared a unique SSL certificate spoofing Microsoft on port 443 (SHA1 fingerprint: 0f6afc6e4e383883a6308fcf8d84b14a5bf4ccaf). This certificate has multiple links to wider Chinese state-sponsored cyber espionage activity and is discussed in further detail below.

ShadowPad C2 IP Address	ASN	First Seen
14.43.108[.]22	AS4766	Aug 27, 2021
210.123.140[.]200	AS45361	Sep 15, 2021
112.171.218[.]39	AS4766	Jan 12, 2022
114.35.191[.]224	AS3462	Jan 12, 2022
59.10.140[.]47	AS4766	Jan 13, 2022
121.151.212[.]101	AS4766	Oct 18, 2021
119.200.211[.]197	AS4766	Feb 8, 2022
124.216.159[.]70	AS4766	Feb 23, 2022
211.184.160[.]108	AS4766	Feb 28, 2022

Table 1: Sample list of ShadowPad C2 servers linked to TAG-38 targeting of Indian power sector and additional victims

Overlaps With Other China-Nexus Threat Activity

While investigating the TAG-38 intrusion activity, we uncovered multiple links to other suspected Chinese state-sponsored activity. Of note, the targeting and use of ShadowPad is consistent with previously reported RedEcho activity, and this latest activity also includes a repeated SLDC victim. However, there were distinct differences in the infrastructure TTPs used in this latest campaign, and at this time we have not identified sufficient technical evidence tying these 2 activity groups together beyond the common targeting sets and capability use.

The use of a shared SSL certificate (SHA1 fingerprint 0f6afc6e4e383883a6308fcf8d84b14a5bf4ccaf) exhibited on several TAG-38 servers was also notable. This SSL certificate was also identified historically on a few dozen other servers with links to Chinese cyber espionage activity. For example, one of the IP addresses historically exhibiting this certificate, 185.243.41[.]240, concurrently hosted several domains attributed to the group we track as TAG-26 referenced earlier in this report (including supership.dynv6[.]net, supermarket.ownip[.]net, and greatsong.soundcast[.]me). At this time, we believe it is unlikely that the use of this certificate is exclusive to a single activity group. This is based on wider context such as differing targeting patterns, infrastructure TTPs, and capability use linked to the infrastructure historically sighted exhibiting this certificate, which may instead be indicative of a shared capability.

Subject:	CN=www.microsoft.com
Issuer:	CN=www.microsoft.com
Decimal:	-305743029826360656630207947036122410 0
Hex:	0xfdb3290c46b41fb24a0fefd16e565c5c
Validity:	2021-06-07 14:29:51 to 2039-12-31 23:59:59
Names:	www.microsoft.com
SHA-256:	B63e14d24e0893f85e80b4b94ad0bd800d6e105 70dc93ec56bbe75cd665385b0
SHA-1:	0f6afc6e4e383883a6308fcf8d84b14a5bf4ccaf
MD5:	d06cc3e6f5673b2e9bfdac55944109a5

Figure 6: Shared SSL certificate linked to TAG-38 and wider Chinese cyber espionage activity

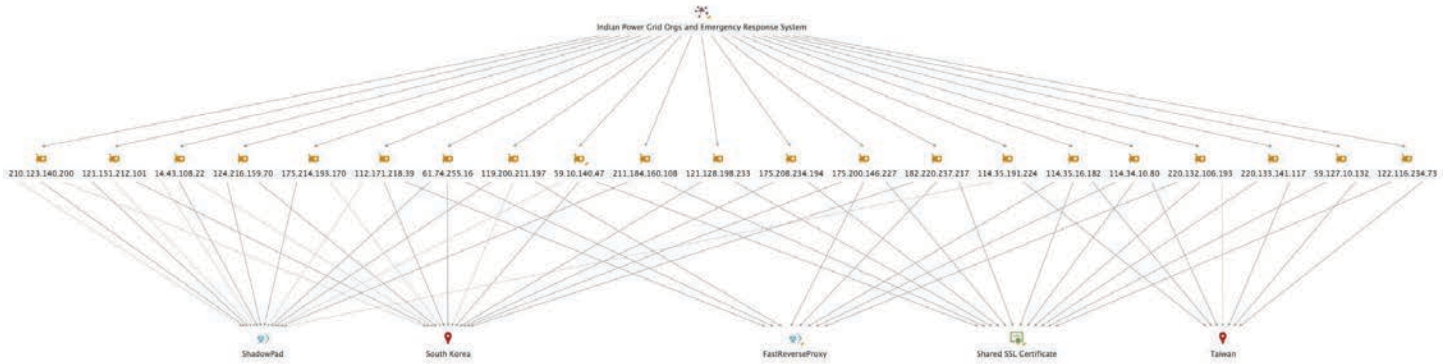

Figure 5: Maltego chart of TAG-38 infrastructure clustering

Mitigations

We recommend that users conduct the following measures to detect and mitigate activity associated with TAG-38 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 TAG-38 and Chinese state-sponsored threat activity groups, such as ShadowPad. Recorded Future clients should alert on and block these C2 servers to allow for detection and remediation of active intrusions.
- Monitor for consistent anomalous outbound traffic from your network to unusual servers, such as compromised DVR/IP camera systems in this case, which may be indicative of malware beaconing activity.
- Ensure software and firmware associated with IOT devices, such as DVR/IP camera systems, are kept up to date. Always change any default passwords to a strong, complex password and turn on two-factor authentication (2FA) if available. Where possible, avoid exposing these devices directly to the internet.
- 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.

Outlook

Recorded Future continues to track Chinese state-sponsored activity groups targeting a wide variety of sectors globally. A large majority of this conforms to longstanding cyber espionage efforts, such as targeting of foreign governments, surveillance of dissident and minority groups, and economic espionage. However, the coordinated effort to target Indian power grid assets in recent years is notably distinct from our perspective and, given the continued heightened tension and border disputes between the two countries, we believe is a cause for concern.

Based on the complexity present across national critical infrastructure systems, this often necessitates lengthy reconnaissance operations to better understand the inner workings of these systems, both in a technological and a physical sense. This is reflected in publicly documented targeted intrusion activity targeting industrial control system (ICS) networks historically, which can often span years. At this time, we have not identified evidence of compromise of ICS networks by TAG-38 operators from our visibility, although we cannot discount this possibility. Given the prolonged targeting of both SLDCs and RLDCs within India, first from RedEcho and now in this latest TAG-38 activity, we believe this targeting is a strategic priority for these actors and is likely to continue.

Appendix A — Indicators

Readers can access the indicators listed below in our public Insikt Group Github repository: https://github.com/Insikt-Group/Research **(Continued Targeting of Indian Power Grid Assets by China State-sponsored Activity Group - March 2022).**

Note: We have observed a portion of the compromised infrastructure listed below indiscriminately scanning the internet outside of the First Seen/Last Seen dates associated with TAG-38 activity. Careful consideration should be given to these dates when analyzing any communications to these network indicators within your environment. The malicious activity described in this report consists of consistent long-term outbound network traffic to these nodes indicative of malware beaconing, not inbound scanning or brute forcing activity.

Network Indicator	First Seen	Last Seen
14.43.108[.]22	Aug 27, 2021	Dec 31, 2021
59.10.140[.]47	Jan 13, 2022	Feb 2, 2022
59.127.10[.]132	Feb 12, 2022	Mar 15, 2022
61.74.255[.]16	Feb 25, 2022	Mar 15, 2022
122.116.165[.]62	Feb 23, 2022	Mar 15, 2022
112.171.218[.]39	Jan 12, 2022	Feb 13, 2022
114.34.10[.]80	Feb 17, 2022	Mar 15, 2022
114.35.16[.]182	Mar 1, 2022	Mar 20, 2022
114.35.191[.]224	Jan 12, 2022	Feb 22, 2022
119.200.211[.]197	Feb 8, 2022	Mar 3, 2022
121.128.198[.]233	Feb 17, 2022	Mar 13, 2022
121.151.212[.]101	Oct 18, 2021	Dec 23, 2021
122.116.234[.]73	Dec 23, 2021	Mar 13, 2022
124.216.159[.]70	Feb 23, 2022	Mar 21, 2022
175.200.146[.]227	Dec 29, 2021	Feb 17, 2021
175.208.234[.]194	Feb 18, 2022	Feb 21, 2022
175.214.193[.]170	Feb 12, 2022	Mar 21, 2022
182.220.237[.]217	Feb 17, 2022	Mar 22, 2022
210.123.140[.]200	Sep 15, 2021	Mar 2, 2022
211.184.160[.]108	Feb 28, 2022	Mar 22, 2022
220.132.106[.]193	Feb 17, 2022	Mar 15, 2022
220.133.141[.]117	Feb 17, 2022	Mar 15, 2022
Shared SSL Certificate (SHA1 Fingerprint): 0f6afc6e4e383883a6308fcf8d84b14a5bf4ccaf		

Appendix B — MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Compromise Infrastructure	T1584
Command and Control: Proxy: Multi-hop Proxy	T1090.003
Command and Control: Application Layer Protocol - Web Protocols	T1071
Exfiltration: Exfiltration Over C2 Channel	T1041

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

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