

CYBER
THREAT
ANALYSIS

CHINA

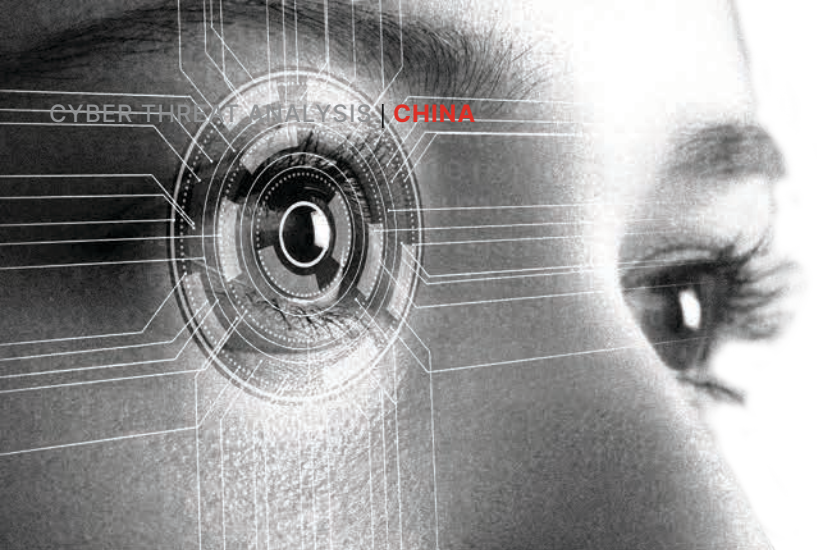
Recorded Future®

By Insikt Group®

September 21, 2021



China-Linked Group TAG-28 Targets India's "The Times Group" and UIDAI (Aadhaar) Government Agency With Winnti Malware



Executive Summary

India continues to bear the brunt of hostile cyber operations from Chinese state-sponsored groups. Earlier this year, Insikt Group [documented](#) a RedEcho campaign targeting India's critical national infrastructure following a rapid deterioration in bilateral relations after both countries clashed on the China-India border. We also recently identified renewed RedFoxytrot operations targeting an Indian state-owned enterprise involved in the nuclear, space, and defense sectors.

Following this theme of Chinese targeting of Indian entities, we have identified further suspected intrusions targeting the Indian media conglomerate Bennett Coleman And Co Ltd (BCCL), commonly known as "The Times Group"; the Unique Identification Authority of India (UIDAI); and the Madhya Pradesh Police department. The UIDAI is the Indian government agency responsible for the national identification database, more commonly called "Aadhaar", which contains private biometric information for over 1 billion Indian citizens. These intrusions were conducted by an activity group we track using a temporary designation, TAG-28¹.

¹ Insikt Group publicly names a new threat activity group or campaign, such as RedFoxytrot, typically 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-28, 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.

Chinese state-sponsored intrusions targeting news outlets is not a recent phenomenon. In 2013, the New York Times, the Washington Post, and Bloomberg News were [targeted](#) by a Chinese group in a widespread intelligence-gathering operation following a series of published articles that were perceived as presenting China unfavorably. Subsequently in 2014, pro-democracy news outlets in Hong Kong were [targeted](#) during the Umbrella Movement protests. TAG-28's Winnti campaign targeting BCCL is the latest in a long line of targeted intrusions against international media outlets.

Key Judgments

- TAG-28 highly likely targeted UIDAI due to its ownership of the Aadhaar database. Bulk personally identifiable information (PII) data sets are valuable to state-sponsored threat actors. Likely uses of such data include, but are not limited to, identifying high-value targets such as government officials, enabling social engineering attacks, or enriching other data sources.
- Given the reach of The Times Group publications and their consistent reporting on the "[India China war](#)", TAG-28's targeting of BCCL is likely motivated by wanting access to journalists and their sources as well as pre-publication content of potentially [damaging](#) articles focusing on China or its leadership.
- It is less likely that TAG-28 would gain access to media entities to interfere with publishing platforms by changing or disrupting articles supporting Chinese [information](#) operations.
- As of early August 2021, Recorded Future data shows a 261% increase in the number of suspected state-sponsored Chinese cyber operations targeting Indian organizations and companies already in 2021 compared to 2020. This follows an increase of 120% between 2019 and 2020, demonstrating China's growing strategic interest in India over the past few years.

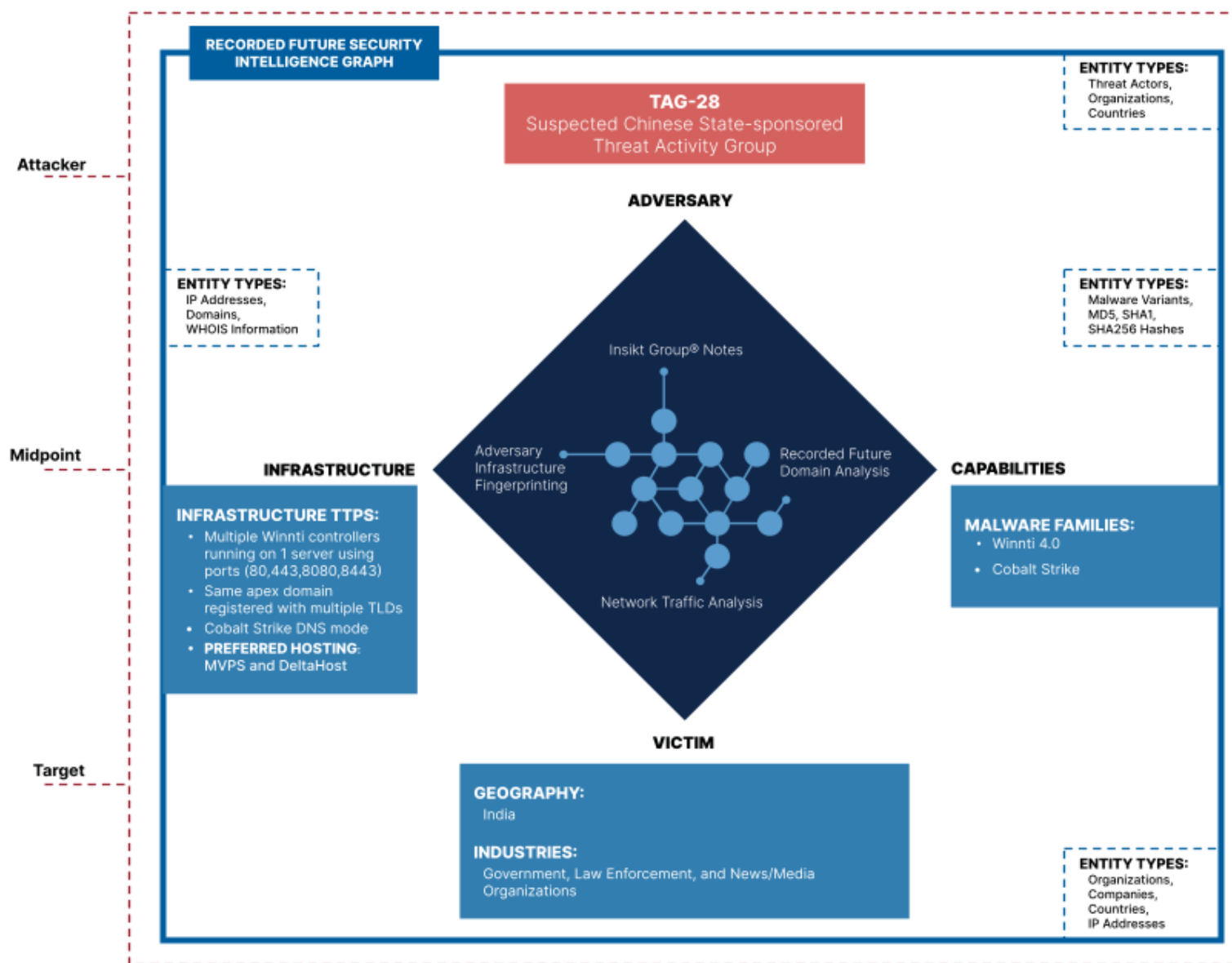


Figure 1: Diamond model representation of TAG-28 TTPs (Source: Recorded Future)

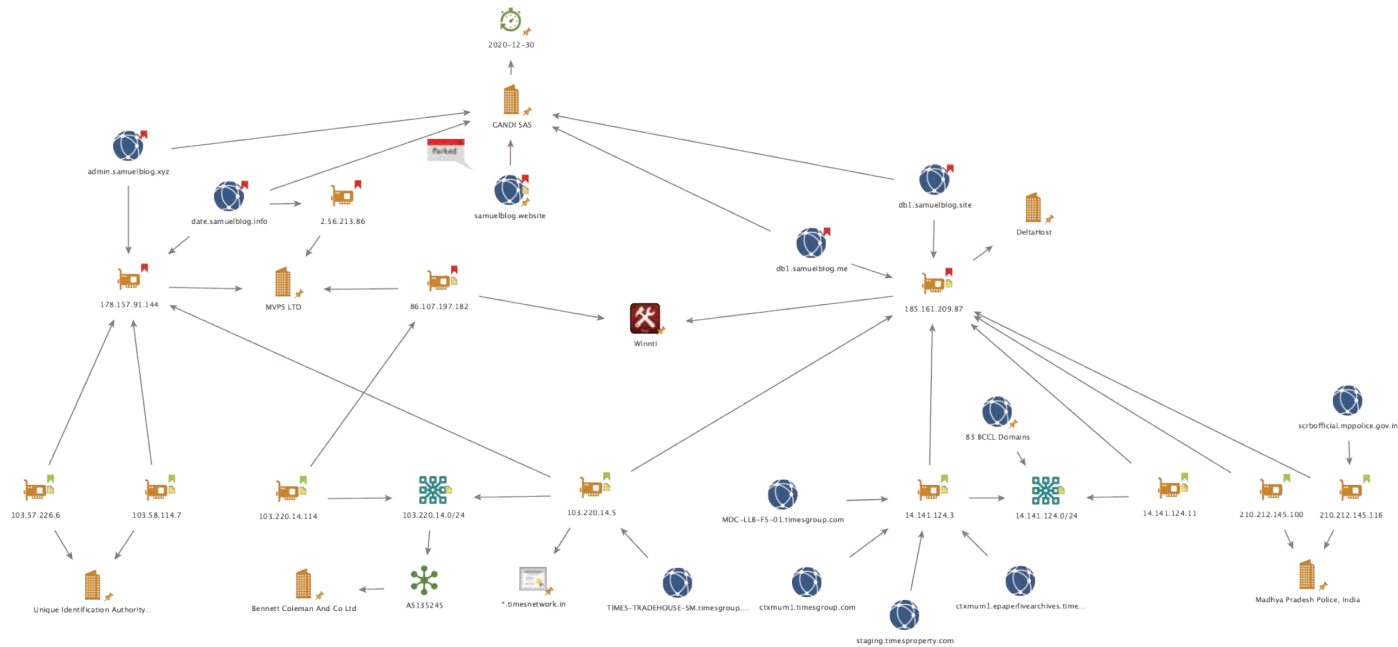


Figure 2: TAG-28 infrastructure used to communicate with BCCL (Source: Recorded Future)

Threat Analysis

Since early 2020, we have observed a large increase in suspected targeted intrusion activity against Indian organizations from Chinese state-sponsored groups, as illustrated through Insikt Group reporting on [RedEcho](#), [RedFoxtrot](#), TAG-26², and TAG-27³.

We used a combination of adversary command and control (C2) detection techniques and Recorded Future Network Traffic Analysis (NTA) data to identify patterns of suspicious network traffic between 2 [Winnti](#) malware C2 servers and infrastructure registered to BCCL.

Targeting of Bennett Coleman And Co Ltd

Between February and August 2021, Insikt Group identified 4 IPs assigned to BCCL in sustained and substantial network communications with 2 [Winnti](#) C2 servers (185.161.209[.]87 and IP 86.107.197[.]182) and a third probable Cobalt Strike C2 178.157.91[.]144. Although we cannot confirm what data specifically was accessed, we observed approximately 500 MB of data being exfiltrated from the BCCL network to the malicious infrastructure.

The identified targeted infrastructure is likely operated by BCCL for the following reasons:

- 2 of the targeted IPs, 103.220.14[.]5 and 103.220.14[.]114, are [advertised](#) by autonomous system (AS) [AS135245](#), [registered](#) to Bennett Coleman And Co Ltd.
- Multiple BCCL domain names are associated with 2 of the targeted IPs (103.220.14[.]5 and 14.141.124[.]3).
- Targeted IP 103.220.14[.]5 serves an SSL [certificate](#) for BCCL domain *.timesnetwork[.]in.
- A CheckPoint firewall device using IP 103.220.14[.]5 on TCP port 264 [returns](#) the device hostname TIMES-TRADEHOUSE-SM.timesgroup[.]com.
- A likely DNS resolver using IP 14.141.124[.]3 on UDP port 53 returns the hostname MDC-LLB-F5-01.timesgroup[.]com.

BCCL, commonly known as “The Times Group”, is a privately owned, Mumbai-headquartered multimillion-dollar company that publishes one of the world’s largest English-language newspapers by circulation — The Times of India. BCCL operates across multiple mediums, including publishing, television, internet, and radio. The Times of India and its subsidiaries frequently [publish](#) analyses on India-China [tensions](#), and in early March 2021, they were among several Indian media outlets that [covered](#) Insikt Group’s public reporting of RedEcho targeting the Indian power sector.


² Only [available](#) to Recorded Future clients.

³ Only [available](#) to Recorded Future clients.

Indian Navy undertaking mega exercise in Indian Ocean Region

PTD - Last Updated: [Client LP](#) Feb 10, 2021, 08:14 PM IST

Synopsis
The exercise is taking place at a time China has been making increasing forays into the Indian Ocean region as part of its offensive military manoeuvre.



CELEBRATE Summer!
Get your summer fix with this complete guide

IN THE SPOTLIGHT
Want to invest in cryptocurrency? Here's a complete guide

RELATED MOST READ MOST SHARED

- Chinese rocket debris lands in Indian Ocean, draws criticism from NASA
- Can China dominate the Indian Ocean?
- Foreign powers should not bring their conflicts to Indian Ocean Region: Maldives
- Not surprising that China operating in Indian Ocean: Indian Navy chief
- UK's carrier strike group enters Indian Ocean, to conduct war game with Indian Navy


New Delhi: The **Indian Navy** is carrying out a mega war game involving almost all operational assets like warships, submarines and aircraft over a vast geographical expanse in the **Indian Ocean Region** to test the force's

Figure 3: *Indian Navy undertaking exercise in Indian Ocean Region*: this article describes a planned Indian naval exercise that was due to take place when China was making increasing forays into the Indian Ocean region as part of its military exercises. Published February 10, 2021. (Source: [India Times](#))

View: China, Turkey and Pakistan's unholy nuclear nexus and its global ramifications

By Dr. Nalin Kumar Mohapatra, ET CONTRIBUTORS - Last Updated: Feb 11, 2021, 01:23 PM IST

Synopsis
As has been served by US Office of the Secretary of Defense in its annual report to the Congress, Military and Security Developments Involving the People's Republic of China 2020, "PLA to develop the capability to project power outside China's borders and immediate periphery to secure the PRC's growing overseas interests and advance its foreign policy goals."



Do also read the rejoinder by Sakir Ozkan Torunlar, Ambassador of Turkey to India, at the end of the piece.

NEW DELHI: The existing unholy nexus among **China**, **Turkey** and **Pakistan** in the clandestine nuclear program is posing a serious threat to both regional and global security. What is required is that international institutions like the UN and IAEA take strong punitive measures against Beijing, Ankara and Islamabad for their illegal and clandestine activities in the nuclear weaponisation process.

Along with the Covid-19 crisis which is posing a threat to global security, another issue which is causing equal alarm and concerns in the global community is the nexus between Turkey and Pakistan, two rogue states in the field of nuclear weaponisation process. Along with these two, China and North Korea are also involved in the illicit transfer of nuclear technologies

China's President Xi Jinping shakes hands with Pakistan's Prime Minister Imran Khan before a meeting at the Great Hall of the People on April 28, 2019 in Beijing, China.

Unlock your blog's true revenue potential
WordStream Monitor Site Speed and More
GET STARTED

IN THE SPOTLIGHT
Want to invest in cryptocurrency? Here's a complete guide

RELATED MOST READ MOST SHARED

- China must honour legally binding UNCLOS verdict on South China Sea
- Why is China facing record floods?
- Australia takes China to WTO
- China says US revoking of China apps ban a 'positive step'
- China announces Didi cybersecurity investigation
- China challenge for India, the world

Figure 4: *View: China, Turkey and Pakistan's unholy nuclear nexus and its global ramifications*: this article calls out China's nuclear relationships with Turkey and Pakistan as a serious threat to global security and calls for strong punitive measures against Beijing. The article also cites that in February 2020, the Indian Navy intercepted a ship destined for Pakistan from China with hardware believed to be used for nuclear industries. Published February 11, 2021. (Source: [India Times](#))

On multiple occasions (1,2), Chinese state-sponsored groups (APT41, APT12) have targeted the media sector, perhaps most prominently in 2013 when APT12 [compromised](#) The New York Times. Based on comprehensive reporting, it is also [likely](#) that APT41 has an operational scope to track individuals and conduct surveillance of media entities. The New York Times [suggests](#) the timing of the 2013 APT12 attack coincided with reporting on Chinese leadership figures, pointing to a potential flashpoint.

The majority of the observed exfiltration activity coincided with [reports](#) in The Economic Times of a US Navy "freedom patrol" in the Indian Ocean. The Economic Times (a subsidiary of The Times Group) published 2 articles on its "[India China war](#)" subsection just days before Insikt Group detected the initial intrusion activity targeting BCCL. Both of the articles, shown in figures 3 and 4, as well as more recently [published](#) pieces, could be viewed as being antagonistic towards the Chinese government. While the timing of the initial intrusion and exfiltration activity coinciding with notable naval-related articles is circumstantial evidence of possible intent, it remains plausible that TAG-28's objectives may have included targeting the media group to garner insight into Indian ocean naval matters or perceived anti-China reporting.

Targeting of the Unique Identification Authority of India

While investigating the infrastructure used in the BCCL compromise, we identified an ongoing compromise of the UIDAI, which oversees India's Aadhaar ID card system. Between June 10 and at least July 20, 2021, 2 IPs registered to UIDAI were observed communicating with the same suspected Cobalt Strike C2 server used to target BCCL, 178.157.91[.144]. Data transfer sizes were comparatively modest from the UIDAI network based on our visibility. Less than 10 MB of data was egressed with an ingress of almost 30 MB, possibly indicating the deployment of additional malicious tooling from the attacker infrastructure.

UIDAI is the Indian government agency responsible for the Aadhaar national identification database. It contains private, identifying, and biometric information for over 1 billion Indian citizens. [Some view](#) the Aadhaar database as controversial: the sheer amount of personal data held by the system makes it an attractive target to both nation-state and criminally motivated adversaries. The Aadhaar system has a history (1, 2, 3) of data leaks and compromise, including [rogue](#) software exploiting the system to create false identity cards and an unsecured application programming interface (API) giving complete visibility of the database.

TAG-28 likely targeted UIDAI due to its ownership of the Aadhaar database. Large PII data sets are valuable to both nation-state and criminal threat actors for multiple purposes, including for potentially identifying high-value intelligence targets such as government officials, enabling surveillance, conducting social engineering attacks, or enriching other data sources.

Targeting of Madhya Pradesh Police

Using Recorded Future NTA data, we [identified](#) a Madhya Pradesh Police (MPP) IP communicating with Winnti C2 IP 185.161.209[.]87 over port 80 on June 1, 2021. The MPP IP serves a State Crime Records Bureau (SCRB) website (scrbofficial.mppolice.gov[.]in), which provides links to various web and mobile applications operated by SCRB. Insikt Group later observed additional network activity between another SCRB IP, 210.212.145[.]100, and 185.161.209[.]87, starting July 27 to at least August 9, 2021. Based on limited visibility, we observed less than 5 MB of data transfer between the MPP and the Winnti server during the considered time frame.

Madhya Pradesh Chief Minister Shivraj Singh Chouhan was [critical](#) of China after the [violent](#) border clashes with Chinese troops in the Ladakh region in June 2020, [calling](#) for the state's residents to boycott Chinese products. Citizens and news outlets were [quick](#) to point out a 2016 tweet in which Chouhan compared India's ruling Bharatiya Janata Party (BJP) to the Chinese Communist Party (CCP), stating that there were "tremendous similarities between the two parties", which shows his clear change in stance on China.

Malware and Infrastructure

Insikt Group identified 2 Winnti C2s (185.161.209[.]87 and 86.107.197[.]182) and a probable Cobalt Strike C2 (178.157.91[.]144) operated by TAG-28.

Winnti malware has historically been used by several Chinese state-sponsored groups, including APT41/Barium and APT17, and is [commonly associated](#) with activity linked to multiple groups of loosely connected private contractors operating on behalf of China's Ministry of State Security (MSS). In September 2020, the US Department of Justice (DoJ) charged 5 Chinese nationals linked to APT41 that had access to Winnti malware for

conducting widespread intrusion operations targeting over 100 victims globally. Clustering all activity featuring the use of the Winnti malware to a single "Winnti" activity group is insufficient given the shared capability across different groups and the varying targeting remits and modus operandi of Winnti users.

C2 IP	First Identified	Ports	Hosting Provider
Winnti 185.161.209[.]87	March 11, 2021	80, 443, 8080, 8443	Zemlyaniy Dmitro Leonidovich (DeltaHost)
Winnti 86.107.197[.]182	April 8, 2021	443, 8443	MVPS LTD
Suspected Cobalt Strike 178.157.91[.]144	June 10, 2021	443, 53	MVPS LTD

Table 1: Malicious infrastructure used by TAG-28 in this campaign

Pivoting on the C2 IPs, we identified several linked domains. All of the domains were registered on December 30, 2020 using the registrar Gandi SAS, shared the same apex domain "samuelblog", and used "KE" (denoting Kenya) for the registrant country.

- samuelblog[.]me
- samuelblog[.]site
- samuelblog[.]info
- samuelblog[.]website
- samuelblog[.]xyz

A further 4 subdomains were also identified resolving to the same C2 infrastructure listed in Table 1. Based on the subdomain names, we assess they were likely impersonating hostnames used for database access, admin panel, or other similar services.

Network Traffic Analysis

MAY
31
2021

Potential Exfiltration to Malware C2 Server from 210.212.145.116 to 185.161.209.87 on May 31, 2021

"At least 1.44 MB transferred from 210.212.145.116 on port 27778 to 185.161.209.87 (suspected Winnti C2 Server) on port 80 on May 31, 2021. Domain(s) ns1.v8073.dh.net.ua, v8073.dh.net.ua, db1.samuelblog.site, ...and 1 more resolved to the C2 IP at the time of network traffic. Domain(s) scrbofficial.mppolice.gov.in resolved to the suspected victim IP at the time of network traffic." [View analysis report](#)

Source Recorded Future Network Traffic Analysis on Jun 1, 2021, 18:47 • [Reference Actions](#) • [1+ reference](#)

Figure 5: Recorded Future NTA event involving Madhya Pradesh Police IP and Winnti C2 185.161.209[.]87. (Source: Recorded Future)

Sub Domain	IP Resolved
db1.samuelblog[.]me	185.161.209[.]87
db1.samuelblog[.]site	185.161.209[.]87
date.samuelblog[.]info	2.56.213[.]86
	178.157.91[.]144
admin.samuelblog[.]xyz	178.157.91[.]144

Table 2: TAG-28 C2 subdomains

Cobalt Strike C2 Over DNS

Between January 4 and February 25, 2021, the domain ns1.samuelblog[.]info was likely configured as a Cobalt Strike C2. During this period, an NS record for this domain pointed at date.samuelblog[.]info, which subsequently resolved to 2 IPs, 2.56.213[.]86 and 178.157.91[.]144, both hosted with MVPS Ltd.

Using Passive DNS data, we found several suspicious DNS A record queries for variants of the subdomain api.[data resembling hexadecimal notation].ns1.samuelblog[.]info. Where the hex data was longer than 24 characters, the data was split into runs of 56 characters separated by a period. Further research highlighted several other domains displaying a similar pattern (api.[hex data].ns1.); the majority of IPs resolved by these domains had triggered Cobalt Strike C2 server detections in the Recorded Future Platform. Further to this point, a [tutorial](#) video created by Raphael Mudge, the creator of Cobalt Strike, shows DNS beacon traffic matching the pattern observed above. Given these factors, we determined the suspicious DNS traffic for samuelblog[.]info was likely a result of its use as a Cobalt Strike C2.

Adversary

Based on our visibility, Insikt Group strongly believes TAG-28 is a Chinese state-sponsored threat activity group tasked with gathering intelligence on Indian targets. Our attribution to China is predicated on their use of Winnti malware, which is exclusively shared among several Chinese state-sponsored activity groups, and their targeting of at least 3 distinct Indian organizations in this campaign. As we continue to track TAG-28's operational activity, we will gather additional referential data points that will allow us to build on our current understanding of their capabilities and objectives and highlight overlaps with existing activity groups or graduate TAG-28 to a full-fledged "Red" group like RedEcho or RedFoxtrot. Additional data points, such as persona handles and further upstream attacker infrastructure, would support actor attribution efforts.

Outlook

This research highlights China's continued strategic and tactical interest in India-based organizations, both in the private and public sectors. The 2020 border skirmishes and the subsequent economic sanctions levied by the Indian government banning Chinese mobile applications from the Indian market have resulted in increased tensions between the 2 nations. Gaining access and insight into Indian government departments and organizations will therefore likely remain of paramount interest to Chinese state-sponsored actors for the foreseeable future, as cyber operations play a key role in gathering intelligence on military technology or national security matters, in addition to political and foreign relation developments.

While we cannot confirm the intent behind the observed intrusions, an Indian media entity with broad reach across the Indian population and the Aadhar system both present valuable targets for surveillance, espionage, or [information](#) operations.

Although several China-based groups have migrated over to using Shadowpad and other relatively new malware families, this campaign highlights that established tooling such as Winnti and offensive security tools (OST) like Cobalt Strike still prove highly effective for China-nexus threat groups to conduct targeted intrusions.

Mitigations

Conduct the following measures to detect and mitigate activity associated with TAG-28 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 — external IP addresses and domains associated with TAG-28. Clients can view a list of these in the appendix of the clients-only version of this report.
- Clients can use Recorded Future Hunting Packages to hunt and detect malware families used by TAG-28.
- We proactively detect and log malicious server configurations in our Command and Control Security Control Feed. The C2 list includes malware and tools used by TAG-28 and Chinese state-sponsored threat activity groups, such as Winnti, PlugX, and AXIOMATICASYMPTOTE. Recorded Future clients should alert on and block these C2 servers to allow for detection and remediation of active intrusions.
- Recorded Future Threat Intelligence, Third-Party Intelligence, and SecOps Intelligence [module](#) users can monitor real-time output from NTA and Malware Analysis analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.
- Ensure operating systems and software are up to date with the latest patches to protect against known vulnerabilities.

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 cybercriminals — 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:

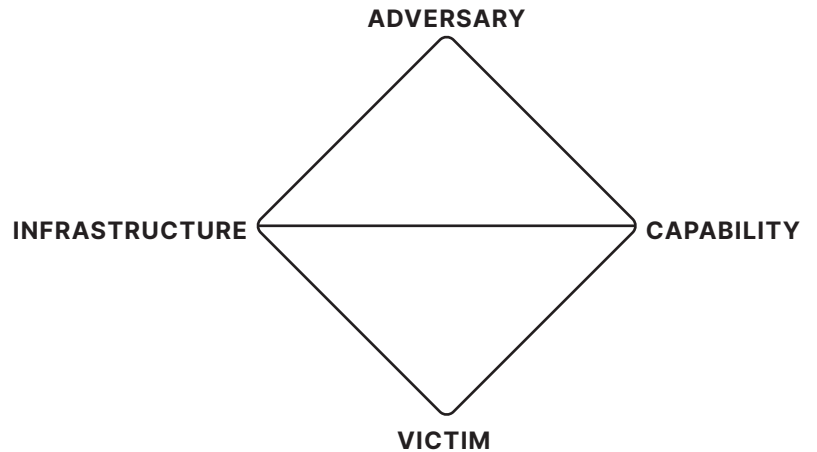
- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors
- Recorded Future-identified, suspected nation-state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other 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 publicly names a new threat activity group or campaign, such as RedFoxtrot, when analysts typically have data corresponding to at least three 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-21 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. We 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 used 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 uses a simple color and phonetic alphabet naming convention for new nation-state threat actor groups or campaigns. The color generally corresponds to that nation's flag colors, 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.



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.