4 Chinese APT Groups Identified Targeting Mail Server of Afghan Telecommunications Firm Roshan

recordedfuture.com/chinese-apt-groups-target-afghan-telecommunications-firm/


Insikt Group

Insikt Group has detected separate intrusion activity targeting a mail server of Roshan, one of Afghanistan's largest telecommunications providers, linked to 4 distinct Chinese state-sponsored threat activity groups. This includes activity we attribute to the Chinese state-sponsored groups RedFoxtrot and Calypso APT, as well as 2 additional clusters using the Winnti and PlugX backdoors that we have been unable to link to established groups at this time. Notably, data exfiltration activity for these intrusions, particularly the Calypso APT activity and the unknown threat actor using the Winnti malware, spiked throughout August and September 2021, coinciding with major geopolitical events such as the withdrawal of US troops and a resurgence in Taliban control. This focus on intelligence gathering targeting one of Afghanistan's largest telecommunications providers is likely in part driven by the Chinese Communist Party's (CCP) purported desire to expand influence within Afghanistan under renewed Taliban rule. The telecommunications firm offers a hugely valuable platform for strategic intelligence collection, be it for monitoring of downstream targets, bulk collection of communication data, as well as the ability to track and monitor individual targets. Moreover, the Chinese government considers the telecommunications sector to be of strategic significance in countries participating in the Belt and Road Initiative.

Timeline of Activity

Insikt Group tracks and regularly reports on a range of Chinese state-sponsored threat activity groups, exemplified by our recent RedFoxtrot reporting in June 2021. One of the methods used to track these groups combines adversary infrastructure detection methods and Recorded Future Network Traffic Analysis (NTA) data. Through our tracking of malicious infrastructure associated with known Chinese state-sponsored actors, we identified multiple concurrent intrusions targeting Roshan over the past year linked to 4 separate activity groups:

- The earliest identified activity targeting Roshan is linked to the suspected Chinese state-sponsored group Calypso APT, and has been ongoing from at least July 2020 to September 2021, and was first reported by Insikt Group in August last year.
- More recently, the same Roshan server was identified communicating with RedFoxtrot PlugX command and control infrastructure from at least March to May 2021. During this time, RedFoxtrot was also identified targeting a second Afghan telecommunications organization.

- Two more clusters were also engaged in the targeting of the same Roshan mail server. These are referred to as the Winnti and PlugX clusters respectively and are outlined further in the sections below. Both of these clusters appear unrelated to each other or the Calypso APT and RedFoxtrot activity, but we have been unable to link them to a tracked activity group at this time.

 ***Figure 1:*** *Timeline of Roshan NTA data exfiltration events versus Afghanistan geopolitical reporting (Source: Recorded Future)*

The targeting of the same organization by activity groups under the same state sponsorship is not unusual, particularly for Chinese adversaries. Many of these groups have separate intelligence requirements and, due to the scale of the Chinese intelligence apparatus, are often not coordinated in their targeting and collection. In this case, as visible in Figure 1, there has been an increase in data exfiltration events associated with the Calypso APT and Winnti intrusions in August and September 2021. This is indicative of both historical strategic collection targeting Afghanistan as well as a further concentration of activity in line with major geopolitical events.

Afghanistan is strategically important to China for several reasons, particularly in the wake of the US withdrawal. For one, the PRC likely seeks to increase its influence within Afghanistan to prevent regional instability and extremism from spreading into the bordering Xinjiang Uyghur Autonomous Region of the PRC, as well as to other Central Asian countries. These issues raise national security concerns and a need to protect PRC interests in the region, including major Belt and Road Initiative (BRI) investments. The US withdrawal also presents the PRC with opportunities for major new BRI-linked and extractive industry projects within Afghanistan.

Technical Analysis

 ***Figure 2:*** *Chart of infrastructure used in Roshan intrusions (Source: Recorded Future)*

As shown in Figure 2, the compromised Roshan server has been identified communicating with a range of adversary C2 infrastructure, particularly associated with the PlugX malware family commonly used by Chinese state-sponsored groups. The section below contains a breakdown of the intrusion activity by group.

RedFoxtrot

In June 2021, Insikt Group reported on RedFoxtrot activity targeting government, defense, and telecommunications organizations across South and Central Asia since at least 2014. We linked this activity group to Unit 69010 of the People's Liberation Army Strategic Support Force (PLASSF) Network System Department (NSD) located in Ürümqi, Xinjiang, through lax operational security employed by a suspected RedFoxtrot operator. The group uses an array of bespoke malware variants commonly associated with Chinese groups, such as IceFog,

QUICKHEAL, and RoyalRoad, as well as other more widely available tools often used by China-linked threat actors, including Poison Ivy, PlugX, and PCShare.
In follow-up analyses in July and September 2021, we identified RedFoxtrot abandoning large amounts of operational infrastructure following public disclosure and reported on several newly identified victims across government and defense sectors in India and Pakistan. RedFoxtrot activity targeting Roshan ceased before our public reporting on the group in June 2021 and was linked to the following PlugX command and control infrastructure:

C2 Domain	Last Seen C2 IP Address	Last Seen Date of Activity
randomanalyze.freetcp[.]com	143.110.250[.]149	April 4, 2021
darkpapa.chickenkiller[.]com	149.28.139[.]86	May 5, 2021
dhsg123.jkub[.]com	159.65.152[.]7 143.110.242[.]139	April 21, 2021

Table 1: *RedFoxtrot PlugX Indicators from Roshan Intrusion*

Calypso APT

In March 2021, Insikt Group reported on the Calypso APT conducting a mass exploitation campaign targeting Microsoft Exchange servers using the ProxyLogon exploit chain (CVE-2021-26855, CVE-2021-27065), alongside several other Chinese state-sponsored groups. One of the PlugX C2 domains highlighted in this activity, www.membrig[.]com, remains active and is linked to ongoing intrusion activity targeting Roshan.

C2 Domain	Last Seen C2 IP Address	Last Seen Date of Activity
www.membrig[.]com	103.30.17[.]20	September 12, 2021

Table 2: Calypso APT indicators from Roshan intrusion

Unknown Winnti Cluster

The Winnti backdoor has historically been used by several Chinese state-sponsored groups, including APT41/Barium, APT17, and most recently a group tracked by Insikt Group as TAG-22. The Winnti backdoor 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, which had access to Winnti malware, with conducting widespread intrusion operations targeting over 100 victims globally.

In relation to the Roshan targeting, we identified a high level of data exfiltration activity from the targeted Roshan server and the Winnti C2 45.76.144[.]44, from at least August 17 to September 12, 2021. We have been unable to link this Winnti C2 infrastructure with a known group, but it is very likely separate from the RedFoxtrot and Calypso APT activity highlighted above.

Unknown PlugX Cluster

Finally, the same Roshan mail server was also identified communicating with an additional PlugX C2 server from April to August 2021. This PlugX C2, 45.86.162[.]135, is linked to the Australia-based PS hosting reseller Crowncloud.

Outlook

Several Chinese state-sponsored groups remain highly active across Central Asia, often operating in an uncoordinated manner, likely due to differing tasking and chains of command. Like other geopolitical flashpoints such as India and the South China Sea, Afghanistan is likely to remain a prime target for Chinese government intelligence collection following the US's withdrawal and the Taliban's takeover. Always a prime target of cyberespionage activity, telecommunications organizations are at particularly high risk within these regions due to the intelligence value of the data they hold. Additionally, the Chinese government considers it a strategic priority to influence the telecommunications sectors of countries participating in the Belt and Road Initiative, giving it increasing leverage in the debate over global internet governance.