ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware

sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/

Aleksandar Milenkoski

Executive Summary

- Threat actors in the cyberespionage ecosystem are engaging in an increasingly disturbing trend of using ransomware as a final stage in their operations for the purposes of financial gain, disruption, distraction, misattribution, or removal of evidence.
- This report introduces new findings about notable intrusions in the past three years, some of which were carried out by a Chinese cyberespionage actor but remain publicly unattributed.
- Our findings indicate that ChamelGang, a suspected Chinese APT group, targeted the major Indian healthcare institution AIIMS and the Presidency of Brazil in 2022 using the CatB ransomware. Attribution information on these attacks has not been publicly released to date.
- ChamelGang also targeted a government organization in East Asia and critical infrastructure sectors, including an aviation organization in the Indian subcontinent.
- In addition, a separate cluster of intrusions involving off-the-shelf tools BestCrypt and BitLocker have affected a variety of industries in North America, South America, and Europe, primarily the US manufacturing sector.
- While attribution for this secondary cluster remains unclear, overlaps exist with past intrusions that involve artifacts associated with suspected Chinese and North Korean APT clusters.

Read the Full Report

Overview

In collaboration with Recorded Future, SentinelLabs has been tracking two distinct activity clusters targeting government and critical infrastructure sectors globally between 2021 and 2023. We associate one activity cluster with the suspected Chinese APT group ChamelGang (also known as CamoFei), while the second cluster resembles previous intrusions involving artifacts linked to suspected Chinese and North Korean APT groups. The majority of the activities we analyzed involve ransomware or data encryption tooling.

ChamelGang

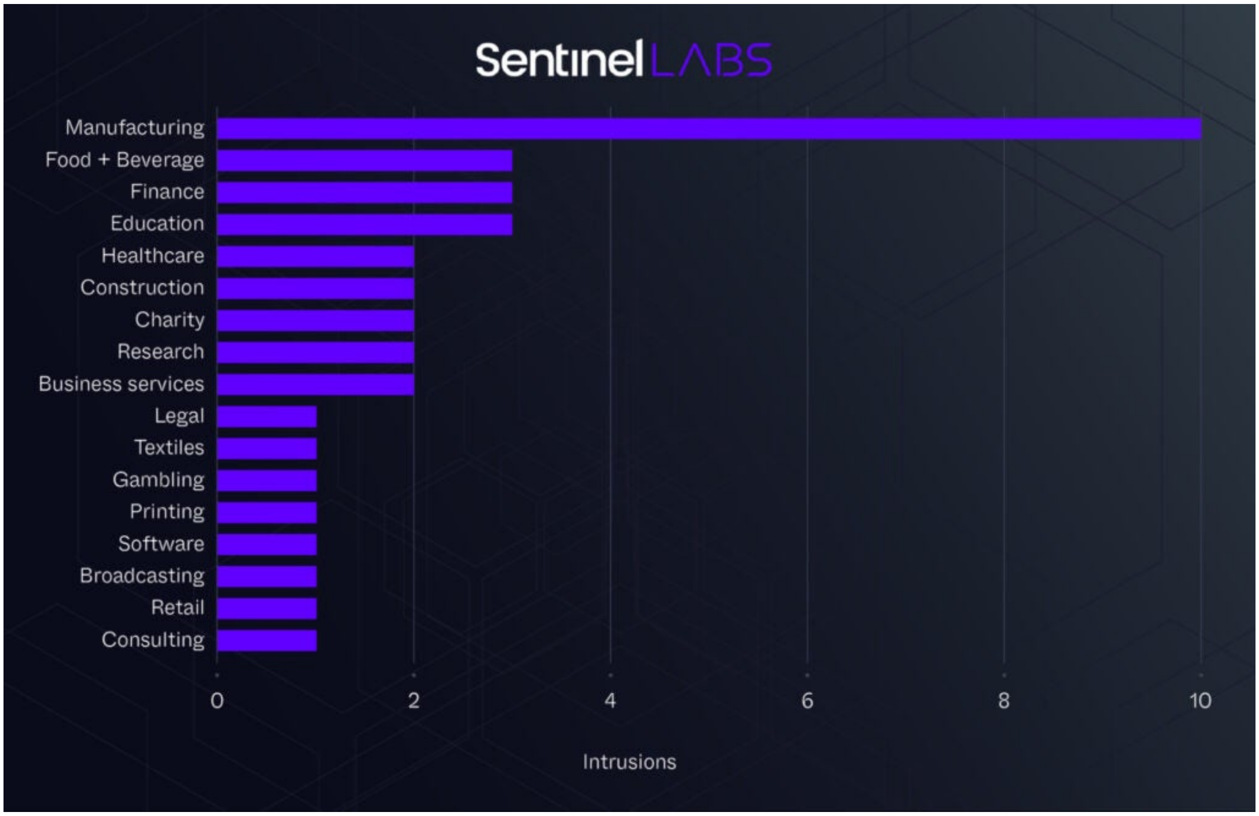
We identified indicators suggesting that in 2023, ChamelGang targeted a government organization in East Asia and an aviation organization in the Indian subcontinent. This aligns with known ChamelGang victimology – previous ChamelGang attacks have impacted critical sectors in Russia, including aviation, as well as government and private organizations in other countries such as the United States, Taiwan, and Japan. The activities we observed involve the use of the group's known TTPs, publicly available tooling seen in previous engagements, and their custom malware BeaconLoader.

Further, we suspect that in late 2022, ChamelGang was responsible for attacks on the Presidency of Brazil and the All India Institute of Medical Sciences (AIIMS), a major Indian healthcare institution. These attacks were publicly disclosed as ransomware incidents and attribution information regarding the perpetrators has never been released. We discovered strong indicators pointing to these institutions as being targeted using ChamelGang's CatB ransomware. TeamT5 associates CatB with ChamelGang based on overlaps in code, staging mechanisms, and malware artifacts such as certificates, strings, and icons found in custom malware used in intrusions attributed to ChamelGang.

BestCrypt & BitLocker

In addition to the ChamelGang activities, we have observed intrusions involving abuse of Jetico BestCrypt and Microsoft BitLocker to encrypt endpoints as a means to demand ransom. BestCrypt and BitLocker are used legitimately for data protection purposes.

Our telemetry data revealed that these intrusions occurred between early 2021 and mid-2023, affecting 37 organizations. The majority of the affected organizations are located in North America, predominantly in the United States, with others in South America and Europe. The manufacturing sector was the most significantly affected, with other sectors, including education, finance, healthcare, and legal, being impacted to a lesser extent.



BestCrypt & BitLocker targets

Our full report provides extensive details, including victimology, discussions on attribution, an overview of the malware and techniques used, as well as a comprehensive list of indicators of compromise.

Ransomware as a Strategic & Operational Tool in Cyber Espionage

This research highlights the strategic use of ransomware by cyberespionage actors for financial gain, disruption, or as a tactic for distraction or misattribution, blurring the lines between cybercrime and cyberespionage.

Misattributing cyberespionage activities as cybercriminal operations can result in strategic repercussions, especially in the context of attacks on government or critical infrastructure organizations. Insufficient information sharing between the local law enforcement organizations that typically handle ransomware cases and intelligence agencies could result in missed intelligence opportunities, inadequate risk assessment, and diminished situational awareness.

We emphasize the importance of sustained exchange of data and knowledge between the different entities handling cybercriminal and cyberespionage incidents, detailed examination of observed artifacts, and analysis of the broader context surrounding incidents involving ransomware. These are crucial towards identifying the true perpetrators, motive, and objectives.

SentinelLabs continues to monitor cyberespionage groups that challenge traditional categorization practices. We remain committed to sharing our insights to equip organizations and other relevant stakeholders with the necessary knowledge to better understand and defend against this threat. We are grateful to Still Hsu from TeamT5 for providing invaluable insights that contributed to our research on the ChamelGang APT group.

Read the Full Report