


Mphasis SOC – Information Security News

Date & Time Issued: 28-Jun-2024, 14:00 IST

Title	New Linux malware is controlled through emojis sent from Discord	
Summary	<ul style="list-style-type: none"> • SentinelLabs and Recorded Future have released a report on cyberespionage groups using ransomware. The report details the activities of ChamelGang, a suspected Chinese threat actor, known for employing CatB ransomware to target high-profile organizations globally. Further, the report highlights a separate, unattributed activity cluster using BestCrypt and Microsoft BitLocker that has similar goals. • A likely China-backed advanced persistent threat (APT) group has been systematically using ransomware to disguise its relatively prolific cyber-espionage operations for the past three years, at least. • According to SentinelOne, what makes ChamelGang's operations noteworthy is its regular use of a ransomware tool called CatB to distract from and conceal its cyber-espionage focus. • Cyberespionage operations disguised as ransomware activities provide an opportunity for adversarial countries to claim plausible deniability by attributing the actions to independent cybercriminal actors rather than state-sponsored entities," the security vendor said in a report shared with Dark Reading. "Furthermore, misattributing cyberespionage activities as cybercriminal operations can result in strategic repercussions, especially in the context of attacks on government or critical infrastructure organizations. • ChamelGang is not the first China-nexus cyberespionage player to use ransomware in this manner. Other examples include APT41 — an umbrella group of multiple smaller subgroups — and Bronze Starlight, whose victims include organizations in the US and multiple other countries. 	
Severity	Medium 	
Attack Vectors	<ul style="list-style-type: none"> • In ChamelGang's case, the threat actor has typically tended to deploy its ransomware toward the end of its missions where covertness is no longer an operational objective, Milenkoski says. Ransomware can be used as a cover for exfiltrating intelligence-relevant data and deflecting blame, so victims of a ransomware attack should not ignore this aspect when responding to an attack, he says: Depending on the potential value of the targeted organization to adversaries from an intelligence perspective, these dimensions of ransomware activities should be considered when assessing the situation. • ChamelGang is a threat actor that others such as Positive Technologies and Team5 have previously identified as focused on data theft and cyber espionage. Positive Technologies reported on the group's activities in September 2021 following a breach investigation at an energy company where the threat actor disguised its malware and infrastructure to look like legitimate Microsoft, Google, IBM, TrendMicro, and McAfee services. • Team5, which tracks the group as Camo Fei, has assessed the threat actor as having been active since at least 2019 and using a variety of malware tools in its campaigns, including Cobalt Strike, DoorMe, IISBeacon, MGDive, and the CatB ransomware tool. Team5's research showed the threat actor is primarily focused on targets in the government sector and, to a lesser extent, the healthcare, telecommunications, energy, water, and high-tech sectors as well. • SentinelOne itself has assessed ChamelGang's current focus on East Asia and the Indian subcontinent as resulting from geopolitical tensions, regional rivalries and a race for technological and economic superiority. The company's investigations showed the group deployed CatB ransomware in its 2022 attacks on India's AIIMS and against the Brazilian government after using tools such as BeaconLoader and Cobalt Strike during earlier phases of the intrusion. • The interest of threat actors in conducting both cyber espionage and financially motivated activities to collect a ransom depends on their objectives when targeting an organization, Milenkoski says. Historically, a common case where threat actors have shown no interest in collecting ransom is when deploying ransomware for disruptive purposes, he says. But we note that interest in ransom payment may represent a cover by itself. 	
Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	No IOCs found.

Recommendations	<ul style="list-style-type: none">• Never trust or open links and attachments received from unknown sources/senders.• Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway. <p>NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.</p>
References	<ul style="list-style-type: none">• https://www.darkreading.com/ics-ot-security/china-nexus-group-using-ransomware-to-disguise-cyber-espionage-activities• https://www.bleepingcomputer.com/news/security/chinese-cyberspies-employ-ransomware-in-attacks-for-diversion/
<p>The information contained in this message is proprietary. It is for Mphasis and its customers only. Copyright © 2023. All rights reserved by Mphasis.</p>	