Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:29:40 UTC

APT group: Bitter

Names	Bitter *(Forcepoint)* T-APT-17 *(Tencent)* TA397 *(Proofpoint)* G1002 *(MITRE)*	
Country	[South Asia]	
Motivation	Information theft and espionage	
First seen	2013	
Description	(Forcepoint) Forcepoint Security Labs recently encountered a strain of attacks that appear to target Pakistani nationals. We named the attack “BITTER” based on the network communication header used by the latest variant of remote access tool (RAT) used. Our investigation indicates that the campaign has existed since at least November 2013 but has remained active until today.	
Observed	Sectors: Energy, Engineering, Government. Countries: Bangladesh, China, India, Pakistan, Saudi Arabia.	
Tools used	ArtraDownloader, BitterRAT, Dracarys.	
Operations performed	Nov 2013	Spear-phishing emails are used to target prospective BITTER victims. The campaign predominantly used the older, relatively popular Microsoft Office exploit, CVE-2012-0158, in order to download and execute a RAT binary from a website. <https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan>
	Jun 2016	Recently, 360 Threat Intelligence Center found a series of targeted attacks against Pakistan targets. Attacker exploited one vulnerability (CVE-2017-12824) of InPage to craft bait documents (.inp). <https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/>

Sep 2018	Starting in September 2018 and continuing through the beginning of 2019, BITTER launched a wave of attacks targeting Pakistan and Saudi Arabia. This is the first reported instance of BITTER targeting Saudi Arabia. Details surrounding these attacks and the three ArtraDownloader variants observed are described below. <https://unit42.paloaltonetworks.com/multiple-artradownloader-variants-used-by-bitter-to-target-pakistan/>
May 2019	The Anomali Threat Research Team discovered a phishing site impersonating a login page for the Ministry of Foreign Affairs of the People's Republic of China email service. When visitors attempt to login to the fraudulent page, they are presented with a pop-up verification message asking users to close their windows and continue browsing. <https://www.anomali.com/blog/suspected-bitter-apt-continues-targeting-government-of-china-and-chinese-organizations#When:19:24:00Z>
Dec 2020	Windows kernel zero-day exploit (CVE-2021-1732) is used by BITTER APT in targeted attack <https://ti.dbappsecurity.com.cn/blog/index.php/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack/>
Aug 2021	Cisco Talos has observed an ongoing malicious campaign since August 2021 from the Bitter APT group that appears to target users in Bangladesh, a change from the attackers' usual victims. <https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html>
May 2022	Bitter APT continues to target Bangladesh <https://www.secuinfra.com/en/techtalk/whatever-floats-your-boat-bitter-apt-continues-to-target-bangladesh/>
Aug 2022	Bitter APT group using "Dracarys" Android Spyware <https://blog.cyble.com/2022/08/09/bitter-apt-group-using-dracarys-android-spyware/>
Apr 2023	Bitter Group Distributes CHM Malware to Chinese Organizations <https://asec.ahnlab.com/en/51043/>
Nov 2024	Hidden in Plain Sight: TA397's New Attack Chain Delivers Espionage RATs <https://www.proofpoint.com/us/blog/threat-insight/hidden-plain-sight-ta397s-new-attack-chain-delivers-espionage-rats>

Information	<https://unit42.paloaltonetworks.com/multiple-artradownloader-variants-used-by-bitter-to-target-pakistan/> <https://www.proofpoint.com/us/blog/threat-insight/bitter-end-unraveling-eight-years-espionage-antics-part-one> <https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two>
MITRE ATT&CK	<https://attack.mitre.org/groups/G1002/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
