Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:42:02 UTC

APT group: Barium

Names	Barium *(Microsoft)* Pigfish *(iDefense)* Brass Typhoon *(Microsoft)* Starchy Taurus *(Palo Alto)*	
Country	China	
Sponsor	State-sponsored	
Motivation	Information theft and espionage	
First seen	2016	
Description	(Microsoft) Barium begins its attacks by cultivating relationships with potential victims—particularly those working in Business Development or Human Resources—on various social media platforms. Once Barium has established rapport, they spear-phish the victim using a variety of unsophisticated malware installation vectors, including malicious shortcut (.lnk) files with hidden payloads, compiled HTML help (.chm) files, or Microsoft Office documents containing macros or exploits. Initial intrusion stages feature the Win32/Barlaiy implant—notable for its use of social network profiles, collaborative document editing sites, and blogs for C&C. Later stages of the intrusions rely upon Winnti for persistent access. The majority of victims recorded to date have been in electronic gaming, multimedia, and Internet content industries, although occasional intrusions against technology companies have occurred. Also see APT 41 and RedGolf, which overlap with Barium.	
Observed	Sectors: Media, Online video game companies, Technology.	
Tools used	Barlaiy, Cobalt Strike, PlugX, Winnti.	
Counter operations	Nov 2017	Microsoft Asks Judge to Take Down Barium Hackers <https://www.courthousenews.com/wp-content/uploads/2017/11/barium.pdf>
Information	<https://threatvector.cylance.com/en_us/home/digitally-signed-malware-targeting-gaming-companies.html>	

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format
