Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:29:17 UTC

APT group: TaskMasters

Names	TaskMasters *(Positive Technologies)*
Country	China
Motivation	Information theft and espionage
First seen	2010
Description	([Positive Technologies]) The main objective of the group is to steal confidential information. The attackers attempt to burrow into corporate information systems for extended periods and obtain access to key servers, executive workstations, and business-critical systems. At one of the attacked companies, the earliest traces of the group's presence on infrastructure dated to 2010. Since the group had obtained full control of some servers and workstations by that time, the initial breach must have occurred much earlier. Most of the attacked companies relate to manufacturing and industry. In total we are aware of compromise of over 30 companies and organizations in various sectors, including: • Manufacturing and industry • Energy • Government • Science and technology • Systems integration • Software development • Geology • Transport and logistics • Real estate • Construction The group attacked companies in a number of countries. A significant number of their targets were located in Russia and the CIS.

Observed	Sectors: Construction, Energy, Government, IT, Manufacturing, Shipping and Logistics, Technology, Transportation and Systems integration and Real estate. Countries: Russia and CIS.	
Tools used	404-Input-shell web shell, ASPXSpy, AtNow, DbxDump Utility, gsecdump, HTran, jsp File browser, Mimikatz, nbtscan, PortScan, ProcDump, PsExec, PsList, pwdump, reGeorg, RemShell, RemShell Downloader.	
Operations performed	May 2021	Chinese APTs attack Russia <https://blog.group-ib.com/task>
Information	<https://www.ptsecurity.com/ww-en/analytics/operation-taskmasters-2019/>	

Last change to this card: 10 August 2021

Download this actor card in PDF or JSON format
