Axiom, Group 72 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:52:55 UTC

APT group: Axiom, Group 72

Names	Axiom *(Novetta)* Group 72 *(Talos)* G0001 *(MITRE)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2008

Description	(Talos) Group 72 is a long standing threat actor group involved in Operation SMN, named Axiom by Novetta. The group is sophisticated, well funded, and possesses an established, defined software development methodology. The group targets high profile organizations with high value intellectual property in the manufacturing, industrial, aerospace, defense, media sectors. Geographically, the group almost exclusively targets organizations based in United States, Japan, Taiwan, and Korea. The preferred tactics of the group include watering-hole attacks, spear-phishing, and other web-based tactics. The tools and infrastructure used by the attackers are common to a number of other threat actor groups which may indicate some degree of overlap. We have seen similar patterns used in domain registration for malicious domains, and the same tactics used in other threat actor groups leading us to believe that this group may be part of a larger organization that comprises many separate teams, or that different groups share tactics, code and personnel from time to time. Though both this group and Winnti Group, Wicked Panda use the malware Winnti, the two groups appear to be distinct based on differences in reporting on the groups' TTPs and targeting. Could be related to APT 17, Deputy Dog, Elderwood, Sneaky Panda and/or APT 20, Violin Panda.	
Observed	Sectors: Aerospace, Defense, Industrial, Manufacturing, Media. Countries: Japan, South Korea, Taiwan, USA.	
Tools used	9002 RAT, BlackCoffee, DeputyDog, Derusbi, Gh0st RAT, HiKit, PlugX, Poison Ivy, Winnti, ZoxRPC, ZXShell.	
Operations performed	2008/2014	Operation "SMN" Axiom is responsible for directing highly sophisticated cyberespionage against numerous Fortune 500 companies, journalists, environmental groups, pro-democracy groups, software companies, academic institutions and government agencies worldwide for at least the last six years. In our coordinated effort, we performed the first ever-private sponsored interdiction against a sophisticated state sponsored advanced threat group. Our efforts detected and cleaned 43,000 separate installations of Axiom tools, including 180 of their top tier implants. <http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf>
Information	<https://blogs.cisco.com/security/talos/threat-spotlight-group-72> <http://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf>	

MITRE ATT&CK	<https://attack.mitre.org/groups/G0001/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
