Velvet Ant - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:51:52 UTC

APT group: Velvet Ant

Names	Velvet Ant *(Sygnia)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2023	
Description	(Sygnia) Velvet Ant is a sophisticated and innovative threat actor. The investigation confirmed the threat actor maintained a prolonged presence in the organization's on–premises network for about three years. The overall goal behind this campaign was to maintain access to the target network for espionage. The threat actor achieved remarkable persistence by establishing and maintaining multiple footholds within the victim company's environment. One of the mechanisms utilized for persistence was a legacy F5 BIG-IP appliance, which was exposed to the internet and which the threat actor leveraged as an internal Command and Control (C&C). After one foothold was discovered and remediated, the threat actor swiftly pivoted to another, demonstrating agility and adaptability in evading detection. The threat actor exploited various entry points across the victim's network infrastructure, indicating a comprehensive understanding of the target's environment.	
Observed	Countries: East Asia.	
Tools used	EarthWorm, ESRDE, PlugX, ShadowPad Winnti, VELVETSTING, VELVETTAP.	
Operations performed	Jul 2024	China-Nexus Threat Group 'Velvet Ant' Exploits Cisco Zero-Day (CVE-2024-20399) to Compromise Nexus Switch Devices – Advisory for Mitigation and Response <https://www.sygnia.co/threat-reports-and-advisories/china-nexus-threat-group-velvet-ant-exploits-cisco-0-day/> <https://www.sygnia.co/blog/china-threat-group-velvet-ant-cisco-zero-day/>
Information	<https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/>	

Last change to this card: 27 August 2024

Download this actor card in PDF or JSON format
