Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:06:18 UTC

APT group: UNC3886

Names	UNC3886 *(Mandiant)* Fire Ant *(Sygnia)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2021	
Description	(Mandiant) Following the discovery of malware residing within ESXi hypervisors in September 2022, Mandiant began investigating numerous intrusions conducted by UNC3886, a suspected China-nexus cyber espionage actor that has targeted prominent strategic organizations on a global scale. In January 2023, Mandiant provided detailed analysis of the exploitation of a now-patched vulnerability in FortiOS employed by a threat actor suspected to be UNC3886. In March 2023, we provided details surrounding a custom malware ecosystem utilized on affected Fortinet devices. Furthermore, the investigation uncovered the compromise of VMware technologies, which facilitated access to guest virtual machines. Investigations into more recent operations in 2023 following fixes from the vendors involved in the investigation have corroborated Mandiant's initial observations that the actor operates in a sophisticated, cautious, and evasive nature. Mandiant has observed that UNC3886 employed several layers of organized persistence for redundancy to maintain access to compromised environments over time. Persistence mechanisms encompassed network devices, hypervisors, and virtual machines, ensuring alternative channels remain available even if the primary layer is detected and eliminated.	
Observed		
Tools used	BOLDMOVE, CASTLETAP, LOOKOVER, MOPSLED, REPTILE, RIFLESPINE, TABLEFLIP, THINCRUST, Tiny SHell, VIRTUALGATE, VIRTUALPIE, VIRTUALPITA, VIRTUALSHINE.	
Operations performed	Late 2021	Chinese Espionage Group UNC3886 Found Exploiting CVE-2023-34048 Since Late 2021

		<https://cloud.google.com/blog/topics/threat-intelligence/chinese-vmware-exploitation-since-2021/>
	2022	Bad VIB(E)s Part One: Investigating Novel Malware Persistence Within ESXi Hypervisors <https://cloud.google.com/blog/topics/threat-intelligence/esxi-hypervisors-malware-persistence>
	Mid 2022	Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation <https://cloud.google.com/blog/topics/threat-intelligence/fortinet-malware-ecosystem/>
	Oct 2022	Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475) <https://cloud.google.com/blog/topics/threat-intelligence/chinese-actors-exploit-fortios-flaw/>
	2023	Cloaked and Covert: Uncovering UNC3886 Espionage Operations <https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations>
	Mid 2024	Ghost in the Router: China-Nexus Espionage Actor UNC3886 Targets Juniper Routers <https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers>
	Early 2025	Fire Ant: A Deep-Dive into Hypervisor-Level Espeonage <https://www.sygnia.co/blog/fire-ant-a-deep-dive-into-hypervisor-level-espionage/>
Information	<https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations> <https://therecord.media/singapore-accuses-chinese-backed-hackers-critical-infrastructure-attacks> <https://www.trendmicro.com/en_us/research/25/g/revisiting-unc3886-tactics-to-defend-against-present-risk.html>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
