Unfading Sea Haze - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:48:11 UTC

APT group: Unfading Sea Haze

Names	Unfading Sea Haze *(Bitdefender)*
Country	China
Motivation	Information theft and espionage
First seen	2018
Description	(Bitdefender) Bitdefender researchers investigated a series of incidents at high-level organizations in countries of the South China Sea region, all performed by the same threat actor we track as Unfading Sea Haze. Based on the victimology and the cyber-attack's aim, we believe the threat actor is aligned with China's interests. As tensions in the region rise, they are reflected in the intensification of activity on behalf of the Unfading Sea Haze actor, which uses new and improved tools and TTPs. We noticed multiple times that the actor was regaining access to the victim's systems either because of improper credential hygiene or because of bad patching strategies of the edge devices and exposed web services. Thus, this publication intends to raise awareness of the importance of respecting essential best practices that ensure security and to share with the community information that could help detect and disrupt Unfading Sea Haze's espionage activities.
Observed	Sectors: Defense, Government. Countries: South China Sea region.
Tools used	DustyExfilTool, EtherealGh0st, FluffyGh0st, InsidiousGh0st, Ps2dllLoader, SerialPktdoor, SharpJSHandler, SharpZulip, SilentGh0st, Stubbedoor, TranslucentGh0st, xkeylog.
Information	<https://blogapp.bitdefender.com/labs/content/files/2024/05/Bitdefender-Report-DeepDive-creat7721-en_EN.pdf>

Last change to this card: 18 June 2024

Download this actor card in PDF or JSON format
