Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:50:01 UTC

APT group: Grayling

Names	Grayling *(Symantec)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2023
Description	(Symantec) A previously unknown advanced persistent threat (APT) group used custom malware and multiple publicly available tools to target a number of organizations in the manufacturing, IT, and biomedical sectors in Taiwan. A government agency located in the Pacific Islands, as well as organizations in Vietnam and the U.S., also appear to have been hit as part of this campaign. This activity began in February 2023 and continued until at least May 2023. The Symantec Threat Hunter Team, part of Broadcom, has attributed this activity to a new group we are calling Grayling. This activity stood out due to the use by Grayling of a distinctive DLL sideloading technique that uses a custom decryptor to deploy payloads. The motivation driving this activity appears to be intelligence gathering.
Observed	Sectors: Government, IT, Manufacturing, Pharmaceutical. Countries: Taiwan, USA, Vietnam and Pacific Islands.
Tools used	Cobalt Strike, Havoc, Mimikatz, NetSpy.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks>

Last change to this card: 13 October 2023

Download this actor card in PDF or JSON format