APT 16, SVCMONDR - Threat Group Cards: A Threat Actor Encyclopedia

APT group: APT 16, SVCMONDR

Names	APT 16 *(Mandiant)* SVCMONDR *(Kaspersky)* G0023 *(MITRE)*
Country	China
Motivation	Information theft and espionage
First seen	2015
Description	(FireEye) Between November 26, 2015, and December 1, 2015, known and suspected China-based APT groups launched several spear-phishing attacks targeting Japanese and Taiwanese organizations in the high-tech, government services, media and financial services industries. Each campaign delivered a malicious Microsoft Word document exploiting the aforementioned EPS dict copy use-after-free vulnerability, and the local Windows privilege escalation vulnerability CVE-2015-1701. The successful exploitation of both vulnerabilities led to the delivery of either a downloader that we refer to as IRONHALO, or a backdoor that we refer to as ELMER.
Observed	Sectors: Financial, Government, High-Tech, Media. Countries: Japan, Taiwan, Thailand.
Tools used	ELMER, IRONHALO, SVCMONDR.
Information	<https://securelist.com/cve-2015-2545-overview-of-current-threats/74828/> <https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0023/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format