APT 16 (Back to overview)

aka: APT16, SVCMONDR

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.

Associated Families

win.elmer win.ironhalo

References

2019 · MITRE · MITRE ATT&CK
Tool description: ELMER
ELMER

2019 · Council on Foreign Relations · Cyber Operations Tracker
APT 16
APT 16

2015-12-21 · Symantec · Kevin Savage
Backdoor.Elmost
ELMER

2015-12-21 · FireEye · Ryann Winters, FireEye Threat Intelligence
The EPS Awakens - Part 2
ELMER IRONHALO EvilPost

2015-12-21 · Symantec · Kevin Savage
Downloader.Ironhalo
IRONHALO

2015-12-16 · FireEye · Genwei Jiang, Dan Caselden, Ryann Winters
The EPS Awakens
IRONHALO APT 16

Credits: MISP Project