APT16

attack.mitre.org/groups/G0023

1. Home
2. Groups
3. APT16

APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations. [1]

ID: G0023

Version: 1.1

Created: 31 May 2017

Last Modified: 12 October 2020

Version Permalink
Live Version

Enterprise Layer

download view

Techniques Used

Domain	ID	Name	Use	
Enterprise	T1584	.004	Compromise Infrastructure: Server	APT16 has compromised otherwise legitimate sites as staging servers for second-stage payloads.[1]

Software

ID	Name	References	Techniques
S0064	ELMER	[1]	Application Layer Protocol: Web Protocols, Commonly Used Port, File and Directory Discovery, Process Discovery

References

1. Winters, R.. (2015, December 20). The EPS Awakens - Part 2. Retrieved January 22, 2016.