APT17

attack.mitre.org/groups/G0025/

APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. [1]

ID: G0025

ⓘ

Associated Groups: Deputy Dog

Version: 1.1

Created: 31 May 2017

Last Modified: 13 October 2020

Version Permalink
Live Version

Associated Group Descriptions

Name	Description
Deputy Dog	[1]

Enterprise Layer

download view

Techniques Used

Domain	ID	Name	Use	
Enterprise	T1583	.006	Acquire Infrastructure: Web Services	APT17 has created profile pages in Microsoft TechNet that were used as C2 infrastructure.[1]
Enterprise	T1585	Establish Accounts	APT17 has created and cultivated profile pages in Microsoft TechNet. To make profile pages appear more legitimate, APT17 has created biographical sections and posted in forum threads.[1]	

Software

ID	Name	References	Techniques
S0069	BLACKCOFFEE	[1]	Command and Scripting Interpreter: Windows Command Shell, File and Directory Discovery, Indicator Removal on Host: File Deletion, Multi-Stage Channels, Process Discovery, Web Service: Bidirectional Communication, Web Service: Dead Drop Resolver

References

1. FireEye Labs/FireEye Threat Intelligence. (2015, May 14). Hiding in Plain Sight: FireEye and Microsoft Expose Obfuscation Tactic. Retrieved January 22, 2016.