Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:46:22 UTC

APT group: DragonOK

Names	DragonOK *(FireEye)* Bronze Overbrook *(SecureWorks)* Shallow Taurus *(Palo Alto)* G0017 *(MITRE)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2015	
Description	DragonOK is a threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, DragonOK is thought to have a direct or indirect relationship with the threat group Moafee. It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, Poison Ivy, FormerFirstRat, NFlog, and NewCT. Kaspersky also found relations between this group and Rancor.	
Observed	Sectors: High-Tech, Manufacturing. Countries: Cambodia, Japan, Russia, Taiwan, Tibet.	
Tools used	FormerFirstRAT, HTran, IsSpace, KHRAT, Mongall, NewCT, NFlog, PlugX, Poison Ivy, Rambo, SysGet, TidePool.	
Operations performed	Jan 2015	This campaign involved five separate phishing attacks, each carrying a different variant of Sysget malware, also known as HelloBridge. The malware was included as an attachment intended to trick the user into opening the malware. All five phishing campaigns targeted a Japanese manufacturing firm over the course of two months, but the final campaign also targeted a separate Japanese high-tech organization. <https://unit42.paloaltonetworks.com/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/>
	2016	In recent months, Unit 42 has observed a number of attacks that we attribute to this group. Multiple new variants of the previously

		discussed sysget malware family have been observed in use by DragonOK. Sysget malware was delivered both directly via phishing emails, as well as in Rich Text Format (RTF) documents exploiting the CVE-2015-1641 vulnerability that in turn leveraged a very unique shellcode. <https://unit42.paloaltonetworks.com/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/>
	Jan 2017	Cybersecurity expert Niklas Femerstrand in an email yesterday pointed out that while servers in several different countries appear to be the origin the attack, it has been linked to the DragonOK campaign. "The DragonOK campaign has previously [in 2014] targeted organizations in Taiwan, Japan, Tibet and Russia, and political organizations in Cambodia since at least January, 2017," he wrote, adding that there are "strong indications" the campaign is "an operation funded by China". <https://www.phnompenhpost.com/national/kingdom-targeted-new-malware>
Information	<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0017/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=shallowtaurus>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
