Icefog, Dagger Panda - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Icefog, Dagger Panda

Names	Icefog *(Kaspersky)* Dagger Panda *(CrowdStrike)* ATK 23 *(Thales)* Red Wendigo *(PWC)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2011
Description	(Kaspersky) “Icefog” is an Advanced Persistent Threat that has been active since at least 2011, targeting mostly Japan and South Korea. Known targets include governmental institutions, military contractors, maritime and shipbuilding groups, telecom operators, industrial and high-tech companies and mass media. The name “Icefog” comes from a string used in the command-and-control server name in one of the samples. The command-and-control software is named “Dagger Three”, in the Chinese language. During Icefog attacks, several other malicious tools and backdoors were uploaded to the victims’ machines, for data exfiltration and lateral movement. The later group RedAlpha has infrastructure overlap with Icefog.
Observed	Sectors: Aerospace, Defense, Government, High-Tech, Maritime and Shipbuilding, Media, Telecommunications, Utilities and others. Countries: Australia, Austria, Belarus, Canada, China, France, Germany, Hong Kong, India, Italy, Japan, Kazakhstan, Malaysia, Maldives, Mongolia, Netherlands, Pakistan, Philippines, Russia, Singapore, South Korea, Sri Lanka, Taiwan, Tajikistan, Turkey, UK, USA, Uzbekistan.
Tools used	8.t Dropper, Dagger Three, Icefog, Javafog, ShadowPad Winnti.

Operations performed	Jan 2014	The Icefog APT Hits US Targets With Java Backdoor Since the publication of our report, the Icefog attackers went completely dark, shutting down all known command-and-control servers. Nevertheless, we continued to monitor the operation by sinkholing domains and nalyzing victim connections. During this monitoring, we observed an interesting type of connection which seemed to indicate a Java version of Icefog, further to be referenced as “Javafog”. <https://securelist.com/the-icefog-apt-hits-us-targets-with-java-backdoor/58209/>
	2015	“TOPNEWS” Campaign Target: Government, media, and finance organizations in Russia and Mongolia.
	2016	“APPER” Campaign Target: Kazach officials.
	2018	“WATERFIGHT” Campaign Target: Water source provider, banks, and government entities in Turkey, India, Kazakhstan, Uzbekistan, and Tajikistan.
	2018	“PHKIGHT” Campaign Target: An unknown entity in the Philippines.
	2018/2019	“SKYLINE” Campaign Target: Organizations in Turkey and Kazakhstan. <https://www.zdnet.com/article/ancient-icefog-apt-malware-spotted-again-in-new-wave-of-attacks/>
Information	<https://media.kaspersky.com/en/icefog-apt-threat.pdf> <https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20133739/icefog.pdf> <https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt>	

Last change to this card: 10 March 2024

Download this actor card in PDF or JSON format
