China Chopper - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:09:35 UTC

Tool: China Chopper

Names	China Chopper CHINACHOPPER SinoChopper
Category	Malware
Type	Backdoor
Description	(Talos) China Chopper is a tool that allows attackers to remotely control the target system that needs to be running a web server application before it can be targeted by the tool. The web shell works on different platforms, but in this case, we focused only on compromised Windows hosts. China Chopper is a tool that has been used by some state-sponsored actors such as Leviathan and Threat Group-3390, but during our investigation we've seen actors with varying skill levels. In our research, we discovered both Internet Information Services (IIS) and Apache web servers compromised with China Chopper web shells. We do not have additional data about how the web shell was installed, but there are several web application frameworks such as older versions of Oracle WebLogic or WordPress that may have been targeted with known remote code execution or file inclusion exploits. China Chopper provides the actor with a simple GUI that allows them to configure servers to connect to and generate server-side code that must be added to the targeted website code in order to communicate. The server-side code is extremely simple and contains, depending on the application platform, just a single line of code. The backdoor supports .NET Active Server Pages or PHP. We cannot be sure if the simplicity of the server code was a deliberate decision on the part of the China Chopper developers to make detection more difficult, but using pattern matching on such as short snippet may produce some false positive detections.

	The China Chopper client communicates with affected servers using HTTP POST requests. The only function of the server-side code is to evaluate the request parameter specified during the configuration of the server code in the client GUI. In our example, the expected parameter name is 'test.' The communication over HTTP can be easily spotted in the network packet captures. China Chopper contains a remote shell (Virtual Terminal) function that has a first suggested command of 'netstat an|find 'ESTABLISHED." and it is very likely that this command will be seen in process creation logs on affected systems.
Information	<https://blog.talosintelligence.com/2019/08/china-chopper-still-active-9-years-later.html> <https://informationonsecurity.blogspot.com/2012/11/china-chopper-webshell.html> <https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html> <https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html> <https://en.wikipedia.org/wiki/China_Chopper>
MITRE ATT&CK	<https://attack.mitre.org/software/S0020/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.chinachopper>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool China Chopper

Changed	Name	Country	Observed	
APT groups				
	APT 31, Judgment Panda, Zirconium		2016-Mar 2024	
	APT 41		2012-Jul 2025	
	Dalbit		2022	
	DragonSpark		2022	
	Emissary Panda, APT 27, LuckyMouse, Bronze Union		2010-Aug 2023	

	Flax Typhoon		2021-Nov 2023	
	Gallium		2018-Jun 2022	
	Gelsemium		2014-2023	
	Hurricane Panda		2013-Mar 2014	
	Iridium		2018-Dec 2018	
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	
	Mustang Panda, Bronze President		2012-Jun 2025	
	Operation Diplomatic Specter		2022	
	ShaggyPanther		2018	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	
	Storm-0558		2023	
	ToddyCat		2020-2024	
	Tortilla	[Unknown]	2021	
	Tropic Trooper, Pirate Panda, APT 23, KeyBoy		2011-Jun 2023	
	UNC215		2019	

20 groups listed (20 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f712900d-e7eb-4873-93b7-eefd7aba61c2