Poison Carp, Evil Eye - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:08:22 UTC

APT group: Poison Carp, Evil Eye

Names	Poison Carp *(Citizen Lab)* Evil Eye *(Volexity)* Earth Empusa *(Trend Micro)* Red Dev 16 *(PWC)* EvilBamboo *(Volexity)* Sentinel Taurus *(Palo Alto)*
Country	China
Motivation	Information theft and espionage
First seen	2018
Description	(Citizen Lab) • Between November 2018 and May 2019, senior members of Tibetan groups received malicious links in individually tailored WhatsApp text exchanges with operators posing as NGO workers, journalists, and other fake personas. The links led to code designed to exploit web browser vulnerabilities to install spyware on iOS and Android devices, and in some cases to OAuth phishing pages. This campaign was carried out by what appears to be a single operator that we call POISON CARP. • We observed POISON CARP employing a total of eight Android browser exploits and one Android spyware kit, as well as one iOS exploit chain and iOS spyware. None of the exploits that we observed were zero days. POISON CARP overlaps with two recently reported campaigns against the Uyghur community. The iOS exploit and spyware we observed was used in watering hole attacks reported by Google Project Zero, and a website used to serve exploits by POISON CARP was also observed in a campaign called “Evil Eye” reported by Volexity. The Android malware used in the campaign is a fully featured spyware kit that has not been previously documented. • POISON CARP appears to have used Android browser exploits from a variety of sources. In one case, POISON CARP used a working exploit publicly released by Exodus Intelligence for a Google Chrome bug that was fixed in source, but whose

	patch had not yet been distributed to Chrome users. In other cases, POISON CARP used lightly modified versions of Chrome exploit code published on the personal GitHub pages of a member of Qihoo 360's Vulcan Team, a member of Tencent's Xuanwu Lab, and by a Google Project Zero member on the Chrome Bug Tracker. • This campaign is the first documented case of one-click mobile exploits used to target Tibetan groups, and reflects an escalation in the sophistication of digital espionage threats targeting the community.	
Observed	Sectors: Tibetan and Uyghur activists as well as those who are interested in their causes. Countries: Australia, Canada, China, Kazakhstan, Syria, Turkey, USA.	
Tools used	ActionSpy, BadBazaar, BADSIGNAL, BADSOLAR, Bourbon, IceCube, IRONSQUIRREL, MOONSHINE, PoisonCarp, Scotch, Whisky and several exploits in iOS, Android and Google Chrome.	
Operations performed	2018	Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs <https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/>
	Jan 2020	Immediately after the publications from Google and Volexity, the Evil Eye threat actor went fairly quiet. They removed their malicious code from compromised websites, command and control (C2) servers were taken down, and various hostnames stopped resolving. This largely remained the case until early January 2020, when Volexity observed a series of new activity across multiple previously compromised Uyghur websites. <https://www.volexity.com/blog/2020/04/21/evil-eye-threat-actor-resurfaces-with-ios-exploit-and-updated-implant/>
	Early 2020	While tracking Earth Empura, also known as POISON CARP/Evil Eye, we identified an undocumented Android spyware we have named ActionSpy. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/>
	2022	Lookout Discovers Long-running Surveillance Campaigns Targeting Uyghurs <https://www.lookout.com/blog/uyghur-surveillance-campaign-badbazaar-moonshine>
	Jun 2023	EvilBamboo Targets Mobile Devices in Multi-year Campaign <https://www.volexity.com/blog/2023/09/22/evilbamboo-targets-

		mobile-devices-in-multi-year-campaign/>
Counter operations	Mar 2021	Taking Action Against Hackers in China <https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/>
Information	<https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/> <https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/> <https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html>	

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format
