APT 31, Judgment Panda, Zirconium

APT group: APT 31, Judgment Panda, Zirconium

Names	APT 31 *(Mandiant)* Judgment Panda *(CrowdStrike)* Zirconium *(Microsoft)* RedBravo *(Recorded Future)* Bronze Vinewood *(SecureWorks)* TA412 *(Proofpoint)* Violet Typhoon *(Microsoft)* Red Keres *(PWC)* G0128 *(MITRE)*	
Country	China	
Sponsor	State-sponsored, Ministry of State Security	
Motivation	Information theft and espionage	
First seen	2016	
Description	FireEye characterizes APT31 as an actor specialized on intellectual property theft, focusing on data and projects that make a particular organization competetive in its field. Based on available data (April 2016), FireEye assesses that APT31 conducts network operations at the behest of the Chinese Government. Also see Hafnium.	
Observed	Countries: Belarus, Canada, Czech, Finland, France, Mongolia, Norway, Russia, UK, USA.	
Tools used	9002 RAT, China Chopper, Gh0st RAT, GrewApacha, HiKit, PlugX, Sakula RAT, Trochilus RAT.	
Operations performed	Summer 2018	Norway says Chinese group APT31 is behind catastrophic 2018 government hack <https://therecord.media/norway-says-chinese-group-apt31-is-behind-catastrophic-2018-government-hack/>

	Aug 2020	New cyberattacks targeting U.S. elections <https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/> <https://www.bleepingcomputer.com/news/security/google-warned-users-of-33-000-state-sponsored-attacks-in-2020/>
	Autumn 2020	Finnish Parliament attackers hack lawmakers' email accounts <https://www.bleepingcomputer.com/news/security/finnish-parliament-attackers-hack-lawmakers-email-accounts/> <https://www.bleepingcomputer.com/news/security/chinese-nation-state-hackers-linked-to-finnish-parliament-hack/>
	Early 2021	Tracing State-Aligned Activity Targeting Journalists, Media <https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists>
	Apr 2021	APT31 new dropper. Target destinations: Mongolia, Russia, the U.S., and elsewhere <https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-new-attacks/>
	Jul 2021	France warns of APT31 cyberspies targeting French organizations <https://www.bleepingcomputer.com/news/security/france-warns-of-apt31-cyberspies-targeting-french-organizations/>
	2022	Czechia blames China for Ministry of Foreign Affairs cyberattack <https://www.bleepingcomputer.com/news/security/czechia-blames-china-for-ministry-of-foreign-affairs-cyberattack/>
	Feb 2022	In February, we detected an APT31 phishing campaign targeting high profile Gmail users affiliated with the U.S. government. <https://www.bleepingcomputer.com/news/security/google-chinese-hackers-target-gmail-users-affiliated-with-us-govt/>
	Apr 2022	Hackers use new malware to breach air-gapped devices in Eastern Europe <https://www.bleepingcomputer.com/news/security/hackers-use-new-malware-to-breach-air-gapped-devices-in-eastern-europe/>
Counter operations	Mar 2024	Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure <https://home.treasury.gov/news/press-releases/jy2205> <https://www.infosecurity-magazine.com/news/uk-blames-china-for-2021-electoral/>

		<https://www.bleepingcomputer.com/news/security/finland-confirms-apt31-hackers-behind-2021-parliament-breach/>
Information	<https://blog.confiant.com/uncovering-2017s-largest-malvertising-operation-b84cd38d6b85> <https://blog.confiant.com/zirconium-was-one-step-ahead-of-chromes-redirect-blocker-with-0-day-2d61802efd0d> <https://threatpost.com/microsoft-offers-analysis-of-zero-day-being-exploited-by-zirconium-group/124600/> <https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html> <https://research.checkpoint.com/2021/the-story-of-jian/> <https://www.sekoia.io/en/walking-on-apt31-infrastructure-footprints/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0128/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
