APT 19, Deep Panda, C0d0so0

APT group: APT 19, Deep Panda, C0d0so0

Names	APT 19 *(Mandiant)* Deep Panda *(CrowdStrike)* Codoso *(CrowdStrike)* C0d0so0 *(CrowdStrike)* Sunshop Group *(FireEye)* TG-3551 *(SecureWorks)* Bronze Firestone *(SecureWorks)* Pupa *(Symantec)* Red Pegasus *(PWC)* Checkered Typhoon *(Microsoft)* G0009 *(MITRE)* G0073 *(MITRE)*
Country	China
Sponsor	A group likely composed of freelancers, with some degree of sponsorship by the Chinese government. (FireEye)
Motivation	Information theft and espionage
First seen	2013
Description	APT 19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. Some analysts track APT19, DarkHydrus, LazyMeerkat, Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens as the same group, but it is unclear from open source information if the groups are the same.

Observed	Sectors: Defense, Education, Energy, Financial, Government, High-Tech, Manufacturing, Pharmaceutical, Telecommunications, Think Tanks and political dissidents and Forbes. Countries: Australia, USA.	
Tools used	C0d0so0, Cobalt Strike, Derusbi, EmpireProject, Fire Chili and a 0-day for Flash.	
Operations performed	Mar 2013	Breach of the US Department of Labor website On April 30, 2013, CrowdStrike was alerted to a strategic web compromise on a US Department of Labor website that was redirecting visitors to an attacker's infrastructure. Eight other compromised sites were also reported to be similarly compromised with the data suggesting that this campaign began in mid-March. <https://www.crowdstrike.com/blog/department-labor-strategic-web-compromise/>
	Early 2014	Breaches of National Security Think Tanks This actor, who was engaged in targeting and collection of Southeast Asia policy information, suddenly began targeting individuals with a tie to Iraq/Middle East issues. This is undoubtedly related to the recent Islamic State of Iraq and the Levant (ISIS) takeover of major parts of Iraq and the potential disruption for major Chinese oil interests in that country. In fact, Iraq happens to be the fifth-largest source of crude oil imports for China and the country is the largest foreign investor in Iraq's oil sector. <https://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/>
	Mar 2014	Breach of the US Office of Personnel Management OPM investigates a breach of its computer networks dating back to March 2014. Authorities trace the intrusion to China. OPM offers employees free credit monitoring and assures employees that no personal data appears to have been stolen. <https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/>
	Mar 2014	Breach of USIS It emerges that USIS, a background check provider for the U.S. Department of Homeland Security, was hacked. USIS offers 27,000 DHS employees credit monitoring through AllClearID (full disclosure: AllClear is an advertiser on this blog). Investigators say Chinese are hackers responsible, and that the attackers broke in by exploiting a vulnerability in an enterprise management software product from SAP.

	<https://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/>
Apr 2014	Breach of health insurance company Anthem <https://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/>
Jul 2014	Sakula Malware to Target Organizations in Multiple Sectors Over the last few months, the CrowdStrike Intelligence team has been tracking a campaign of highly targeted events focused on entities in the U.S. Defense Industrial Base (DIB), healthcare, government, and technology sectors. This campaign infected victims with Sakula malware variants that were signed with stolen certificates. <https://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/>
Nov 2014	Breaches of Australian media organizations ahead of G20 “We started to see activity over the last couple of weeks targeting Australian media organizations and we believe that’s related to the G20,” Dmitri Alperovitch, co-founder of US computer security company CrowdStrike, told the ABC’s 7.30 program. <https://www.abc.net.au/news/2014-11-13/g20-china-affliliated-hackers-breaches-australian-media/5889442>
Dec 2014	Breach of KeyPoint Government Solutions KeyPoint Government Solutions, which took over the bulk of federal background checks after one of its competitors was hacked, also recently suffered a computer network breach, officials said Thursday. <https://www.washingtonpost.com/business/economy/keypoint-suffers-network-breach-thousands-of-fed-workers-could-be-affected/2014/12/18/e6c7146c-86e1-11e4-a702-fa31ff4ae98e_story.html>
Feb 2015	Attack using Forbes.com as Watering Hole Method: Compromise of Forbes.com, in which the site was used to compromise selected targets via a watering hole to a zero-day Adobe Flash exploit. <https://www.darkreading.com/attacks-breaches/chinese-hacking-group-codoso-team-uses-forbescom-as-watering-hole-/d/d-id/1319059>
Apr 2015	Operation “Kingslayer” RSA Research investigated the source of suspicious, observed beaconing thought to be associated with targeted malware. In the course of this tac-tical hunt for unidentified code, RSA discovered a

	sophisticated attack on a software supply-chain involving a Trojan inserted in otherwise legitimate software; software that is typically used by enterprise system administrators. <https://www.rsa.com/content/dam/premium/en/white-paper/kingslayer-a-supply-chain-attack.pdf>
May 2015	Breach of health insurance company Premera Blue Cross Premera Blue Cross, one of the insurance carriers that participates in the Federal Employees Health Benefits Program, discloses a breach affecting 11 million customers. Federal auditors at OPM warned Premera three weeks prior to the breach that its network security procedures were inadequate. <https://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/>
May 2015	Breach of health insurance company Carefirst Blue Cross CareFirst BlueCross BlueShield on Wednesday said it had been hit with a data breach that compromised the personal information on approximately 1.1 million customers. There are indications that the same attack methods may have been used in this intrusion as with breaches at Anthem and Premera, incidents that collectively involved data on more than 90 million Americans. <https://krebsonsecurity.com/2015/05/carefirst-blue-cross-breach-hits-1-1m/>
Jan 2016	Several Watering Hole Attacks <https://unit42.paloaltonetworks.com/new-attacks-linked-to-c0d0s0-group/>
May 2017	Phishing campaign targeting at least seven global law and investment firms. Method: In early May, the phishing lures leveraged RTF attachments that exploited the Microsoft Windows vulnerability described in CVE 2017-0199. Toward the end of May, APT19 switched to using macro-enabled Microsoft Excel (XLSM) documents. In the most recent versions, APT19 added an application whitelisting bypass to the XLSM documents. At least one observed phishing lure delivered a Cobalt Strike payload. <https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html>
Jun 2017	Attacks on Australian law firms and research body <https://www.abc.net.au/news/2017-12-01/chinese-hackers-targeting-australian-law-firms/9213520>

	Mar 2022	Chinese hacking group uses new 'Fire Chili' Windows rootkit <https://www.bleepingcomputer.com/news/security/chinese-hacking-group-uses-new-fire-chili-windows-rootkit/>
Counter operations	Aug 2017	US Arrests Chinese Man Involved With Sakula Malware Used in OPM and Anthem Hacks <https://www.bleepingcomputer.com/news/security/us-arrests-chinese-man-involved-with-sakula-malware-used-in-opm-and-anthem-hacks/>
	Oct 2018	U.S. Indicts Chinese Hacker-Spies in Conspiracy to Steal Aerospace Secrets <https://gizmodo.com/u-s-indicts-chinese-hacker-spies-in-conspiracy-to-stea-1830111695>
	May 2019	Chinese national indicted for 2015 Anthem breach <https://www.cyberscoop.com/anthem-breach-indictment-chinese-national/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0009/> <https://attack.mitre.org/groups/G0073/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
