APT 17, Deputy Dog, Elderwood, Sneaky Panda

Archived: 2026-04-05 18:48:38 UTC

APT group: APT 17, Deputy Dog, Elderwood, Sneaky Panda

Names	APT 17 *(Mandiant)* Tailgater Team *(Symantec)* Elderwood *(Symantec)* Elderwood Gang *(Symantec)* Sneaky Panda *(CrowdStrike)* SIG22 *(NSA)* Beijing Group *(SecureWorks)* Bronze Keystone *(SecureWorks)* TG-8153 *(SecureWorks)* TEMP.Avengers *(FireEye)* Dogfish *(iDefense)* Deputy Dog *(iDefense)* ATK 2 *(Thales)* G0025 *(MITRE)* G0066 *(MITRE)*
Country	China
Sponsor	State-sponsored, Jinan bureau of the Chinese Ministry of State Security
Motivation	Information theft and espionage
First seen	2009
Description	(Symantec) In 2009, Google was attacked by a group using the Hydraq (Aurora) Trojan horse. Symantec has monitored this group's activities for the last three years as they have consistently targeted a number of industries. Interesting highlights in their method of operations include: the use of seemingly an unlimited number of zero-day exploits, attacks on supply chain manufacturers who service the target organization, and a shift to "watering hole" attacks (compromising certain websites likely to be visited by the target organization). The targeted industry sectors include, but are not restricted to; defense, various defense supply chain manufacturers, human rights and non-governmental organizations (NGOs), and IT service providers. These attackers are systematic and re-use components of an infrastructure we have termed the "Elderwood platform". The name "Elderwood" comes from a source code variable used by the attackers. This attack platform enables them to quickly deploy zero-day exploits. Attacks are deployed through spear phishing emails and also, increasingly, through Web injections in watering hole attacks. It is likely the attackers have gained access to the source code for some widely used applications, or have thoroughly reverse-engineered the compiled applications in order to discover these

	vulnerabilities. The vulnerabilities are used as needed, often within close succession of each other if exposure of any of the vulnerabilities is imminent. The scale of the attacks, in terms of the number of victims and the duration of the attacks, are another indication of the resources available to the attackers. Victims are attacked, not for petty crime or theft, but for the wholesale gathering of intelligence and intellectual property. The resources required to identify and acquire useful information—let alone analyze that information—could only be provided by a large criminal organization, attackers supported by a nation state, or a nation state itself. This group appears to be closely associated with Hidden Lynx, Aurora Panda and has infrastructure overlap with RedAlpha. Could also be related to Axiom, Group 72.	
Observed	Sectors: Defense, Education, Energy, Financial, Government, High-Tech, IT, Media, Mining, NGOs and lawyers. Countries: Belgium, China, Germany, Indonesia, Italy, Japan, Netherlands, Switzerland, Russia, UK, USA.	
Tools used	9002 RAT, BlackCoffee, Briba, Comfoo, DeputyDog, Gh0st RAT, HiKit, Jumpall, Linfo, Naid, Nerex, Pasam, Poison Ivy, PlugX, Vasport, Wiarp, ZoxRPC and several 0-days for IE.	
Operations performed	2009	Operation Aurora First publicly disclosed by Google on January 12, 2010, in a blog post, the attacks began in mid-2009 and continued through December 2009. The attack has been aimed at dozens of other organizations, of which Adobe Systems, Juniper Networks and Rackspace have publicly confirmed that they were targeted. According to media reports, Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical were also among the targets. <https://en.wikipedia.org/wiki/Operation_Aurora> <https://googleblog.blogspot.com/2010/01/new-approach-to-china.html>
	Nov 2010	Visitors to Amnesty International's Hong Kong website are being bombarded with a host of lethal exploits, including one that attacks an unpatched vulnerability in Microsoft's Internet Explorer browser, researchers at security firm Websense said. <https://www.theregister.co.uk/2010/11/11/amnesty_international_hosts_ie_exploit/>
	May 2012	Amnesty International UK's website was hacked early this week in an assault ultimately geared towards planting malware onto the PCs of visiting surfers. <https://www.theregister.co.uk/2012/05/11/amnesty_malware_rat/>
	Jul 2012	Breach of Bit9 Bit9, a company that provides software and network security services to the U.S. government and at least 30 Fortune 100 firms, has suffered an electronic compromise that cuts to the core of its business: helping clients distinguish known “safe” files from computer viruses and other malicious software. <https://krebsonsecurity.com/tag/bit9-breach/>
	Aug 2013	Operation “DeputyDog” Target: Organizations in Japan

		Method: Campaign leveraging the then recently announced zero-day CVE-2013-3893. <https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html>
	Nov 2013	Operation “Ephemeral Hydra” Method: Inserting a zero-day exploit into a strategically important website, known to draw visitors that are likely interested in national and international security policy. <https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html>
	Late 2014	FireEye Threat Intelligence and Microsoft Threat Intelligence Center discovered a China-based threat group dubbed APT17 using Microsoft’s TechNet blog for its Command-and-Control (CnC) operation. <https://www.fireeye.com/current-threats/apt-groups/rpt-apt17.html>
	Aug 2017	Operation “RAT Cook” Method: Spear-phishing attack using a Game of Thrones lure. <https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures>
	Sep 2017	Ccleaner supply-chain attack Talos recently observed a case where the download servers used by software vendor to distribute a legitimate software package were leveraged to deliver malware to unsuspecting victims. For a period of time, the legitimate signed version of Ccleaner 5.33 being distributed by Avast also contained a multi-stage malware payload that rode on top of the installation of Ccleaner. <https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>
	Jun 2024	Italian government agencies and companies in the target of a Chinese APT <https://www.tgsoft.it/news/news_archivio.asp?id=1557&lang=eng>
Information	<http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf> <https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/> <https://intezer.com/evidence-aurora-operation-still-active-supply-chain-attack-through-ccleaner/> <https://intezer.com/evidence-aurora-operation-still-active-part-2-more-ties-uncovered-between-ccleaner-hack-chinese-hackers-2/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0025/> <https://attack.mitre.org/groups/G0066/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
