Comment Crew, APT 1 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:35:46 UTC

APT group: Comment Crew, APT 1

Names	Comment Crew *(Symantec)* Comment Panda *(CrowdStrike)* TG-8223 *(SecureWorks)* APT 1 *(Mandiant)* BrownFox *(Symantec)* Group 3 *(Talos)* Byzantine Hades *(US State Department)* Byzantine Candor *(US State Department)* Shanghai Group *(SecureWorks)* GIF89a *(Kaspersky)* G0006 *(MITRE)*
Country	China
Sponsor	State-sponsored, 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398
Motivation	Information theft and espionage
First seen	2006
Description	Also known as APT1, Comment Crew is an advanced persistent threat (APT) group with links to the Chinese military. The threat actors, which were active from roughly 2006 to 2010, managed to strike over 140 US companies in the quest for sensitive corporate and intellectual property data. The group earned their name through their use of HTML comments to hide communication to the command-and-control servers. The usual attack vector was via spear-phishing campaigns utilizing emails which contained documents with names tailored for the potential victims, such as "ArmyPlansConferenceOnNewGCVSolicitation.pdf," or "Chinese Oil Executive Learning From Experience.doc."

	This group may also be responsible for the Siesta campaign.	
Observed	Sectors: Aerospace, Chemical, Construction, Defense, Education, Energy, Engineering, Entertainment, Financial, Food and Agriculture, Government, Healthcare, High-Tech, IT, Manufacturing, Media, Mining, Non-profit organizations, Research, Satellites, Telecommunications, Transportation and Navigation and lawyers. Countries: Belgium, Canada, France, India, Israel, Japan, Luxembourg, Norway, Singapore, South Africa, South Korea, Switzerland, Taiwan, UAE, UK, USA, Vietnam.	
Tools used	Auriga, bangat, BISCUIT, Bouncer, Cachedump, CALENDAR, Combos, CookieBag, Dairy, GDOCUPLOAD, GetMail, GLASSES, GLOOXMAIL, GOGGLES, GREENCAT, gsecdump, Hackfase, Helauto, Kurton, LIGHTBOLT, LIGHTDART, LONGRUN, Lslsass, ManItsMe, MAPIget, Mimikatz, MiniASP, NewsReels, Oceansalt, Pass-The-Hash Toolkit, Poison Ivy, ProcDump, pwdump, Seasalt, ShadyRAT, StarsyPound, Sword, TabMsgSQL, Tarsip, WARP, WebC2, Living off the Land.	
Operations performed	2006/2010	Operation “Seasalt” Target: 140 US companies in the quest for sensitive corporate and intellectual property data. Method: Spear-phishing with malicious documents.
	Mar 2011	Breach of RSA They breached security systems designed to keep out intruders by creating duplicates to “SecurID” electronic keys from EMC Corp’s EMC.N RSA security division, said the person who was not authorized to publicly discuss the matter. <https://www.reuters.com/article/us-usa-defense-hackers/exclusive-hackers-breached-u-s-defense-contractors-idUSTRE74Q6VY20110527> <https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/>
	2011/2012	Hackers Plundered Israeli Defense Firms that Built ‘Iron Dome’ Missile Defense System <https://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/>
	Feb 2014	Operation “Siesta” FireEye recently looked deeper into the activity discussed in TrendMicro’s blog and dubbed the “Siesta” campaign. The tools, modus operandi, and infrastructure used in the campaign present two

		possibilities: either the Chinese cyberespionage unit APT 1 is perpetrating this activity, or another group is using the same tactics and tools as the legacy APT 1. <https://blog.trendmicro.com/trendlabs-security-intelligence/the-siesta-campaign-a-new-targeted-attack-awakens/> <https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html>
	May 2018	Operation “Oceansalt” Target: Oceansalt appears to have been part of an operation targeting South Korea, United States, and Canada in a well-focused attack. A variation of this malware has been distributed from two compromised sites in South Korea. Method: Oceansalt appears to be the first stage of an advanced persistent threat. The malware can send system data to a control server and execute commands on infected machines, but we do not yet know its ultimate purpose. Note: It is possible that this operation was not performed by the actual Comment Crew group (as they are supposedly in jail). <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/> <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf>
Counter operations	May 2014	5 in China Army Face U.S. Charges of Cyberattacks <https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html>
Information	<https://www.symantec.com/connect/blogs/apt1-qa-attacks-comment-crew> <https://en.wikipedia.org/wiki/PLA_Unit_61398>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0006/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
