Patchwork, Dropping Elephant - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:48:03 UTC

APT group: Patchwork, Dropping Elephant

Names	Patchwork *(Cymmetria)* Dropping Elephant *(Kaspersky)* Chinastrats *(Kaspersky)* APT-C-09 *(Qihoo 360)* Monsoon *(Forcepoint)* Quilted Tiger *(CrowdStrike)* TG-4410 *(SecureWorks)* Zinc Emerson *(SecureWorks)* ATK 11 *(Thales)* Thirsty Gemini *(Palo Alto)* Capricorn Organisation *(?)* Maha Grass *(?)* G0040 *(MITRE)*
Country	India
Motivation	Information theft and espionage
First seen	2013
Description	(Cymmetria) Patchwork is a targeted attack that has infected an estimated 2,500 machines since it was first observed in December 2015. There are indications of activity as early as 2014, but Cymmetria has not observed any such activity first hand. Patchwork targets were chosen worldwide with a focus on personnel working on military and political assignments, and specifically those working on issues relating to Southeast Asia and the South China Sea. Many of the targets were governments and government-related organizations. The code used by this threat actor is copy-pasted from various online forums, in a way that reminds us of a patchwork quilt –hence the name we've given the operation.

	In active victim systems, Patchwork immediately searches for and uploads documents to their C&C, and only if the target is deemed valuable enough, proceeds to install a more advanced second stage malware. This group seems to be associated with Confucius.	
Observed	Sectors: Aviation, Defense, Energy, Financial, Government, IT, Media, NGOs, Pharmaceutical, Think Tanks. Countries: Bangladesh, Bhutan, Cambodia, China, Israel, Japan, Myanmar, Nepal, Pakistan, South Korea, Sri Lanka, Turkey, UK, USA and Middle East and Southeast Asia.	
Tools used	AndroRAT, ArtraDownloader, AutoIt backdoor, BADNEWS, Bahamut, Bozok, Brute Ratel, Crypta, LokiBot, NDiskMonitor, PGoShell, PowerSploit, PubFantacy, QuasarRAT, Ragnatela, SocksBot, TINYTYPHON, Unknown Logger, WSCSPL.	
Operations performed	2015	The attack was detected as part of a spear phishing against a government organization in Europe in late May 2016. The target was an employee working on Chinese policy research and the attack vector was a PowerPoint presentation file. The content of the presentation was on issues relating to Chinese activity in the South China Sea. <https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling_Patchwork.pdf>
	Jan 2018	The malicious documents seen in recent activity refer to a number of topics, including recent military promotions within the Pakistan Army, information related to the Pakistan Atomic Energy Commission, as well as Pakistan's Ministry of the Interior. <https://unit42.paloaltonetworks.com/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/>
	Mar 2018	Targeting US Think Tanks In March and April 2018, Volexity identified multiple spear phishing campaigns attributed to Patchwork, an Indian APT group also known as Dropping Elephant. This increase in threat activity was consistent with other observations documented over the last few months in blogs by 360 Threat Intelligence Center analyzing attacks on Chinese organizations and Trend Micro noting targets in South Asia. <https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/>
	Nov 2021	Patchwork APT caught in its own web <https://blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web/>

	Jul 2023	PatchWork's new assault Weapons report — EyeShell Weapons Disclosure <https://medium.com/@knownsec404team/patchworks-new-assault-weapons-report-eyeshell-weapons-disclosure-181833f434be>
	Jul 2024	The Patchwork group has updated its arsenal, launching attacks for the first time using Brute Ratel C4 and an enhanced version of PGoShell <https://medium.com/@knownsec404team/the-patchwork-group-has-updated-its-arsenal-launching-attacks-for-the-first-time-using-brute-ratel-175741987d87>
	Jun 2025	Dropping Elephant APT Group Targets Turkish Defense Industry With New Campaign and Capabilities: LOLBAS, VLC Player, and Encrypted Shellcode <https://arcticwolf.com/resources/blog/dropping-elephant-apt-group-targets-turkish-defense-industry/>
Information		<https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling_Patchwork.pdf> <https://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries> <https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf> <https://securelist.com/the-dropping-elephant-actor/75328/> <https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf> <https://cybleinc.com/2021/01/20/a-deep-dive-into-patchwork-apt-group/>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0040/>
Playbook		<https://pan-unit42.github.io/playbook_viewer/?pb=thirstygemini>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
