Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:24:54 UTC

APT group: Confucius

Names	Confucius *(Palo Alto)* G0142 *(MITRE)*	
Country	India	
Motivation	Information theft and espionage	
First seen	2013	
Description	(Trend Micro) Confucius' campaigns were reportedly active as early as 2013, abusing Yahoo! And Quora forums as part of their command-and-control (C&C) communications. We stumbled upon Confucius, likely from South Asia, while delving into Patchwork's cyberespionage operations. Confucius' operations include deploying bespoke backdoors and stealing files from their victim's systems with tailored file stealers. The stolen files are then exfiltrated by abusing a cloud service provider. Some of these file stealers specifically target files from USB devices, probably to overcome air-gapped environments. This group seems to be associated with Patchwork, Dropping Elephant.	
Observed	Countries: Azerbaijan, Bangladesh, France, India, Indonesia, Iran, Italy, Mongolia, Pakistan, Poland, Russia, Slovakia, Spain, Trinidad and Tobago, UAE, UK, Ukraine, USA and most of the South and Southeast Asian countries, most of the Middle Eastern countries and most of the African countries.	
Tools used	ApacheStealer, Confucius, Hornbill, MY24, sctrls, remote-access-c3, sip_telephone, SunBird, swissknife2, Sneepy.	
Operations performed	Oct 2017	In recent weeks, Unit 42 has discovered three documents crafted to exploit the InPage program. InPage is a word processor program that supports languages such as Urdu, Persian, Pashto, and Arabic. The three InPage exploit files are linked through their use of very similar shellcode, which suggests that either the same actor is behind these attacks, or the attackers have access to a shared builder. <https://unit42.paloaltonetworks.com/unit42-recent-inpage-exploits-lead-multiple-malware-families/>

	Late 2017	Probing Confucius' infrastructure, we came across websites offering Windows and Android chat applications, most likely iterations of its predecessor, Simple Chat Point: Secret Chat Point, and Tweety Chat. We are admittedly uncertain of the extent — and success — of their use, but it's one of the ingredients of the group's operations. <https://blog.trendmicro.com/trendlabs-security-intelligence/deciphering-confucius-cyberespionage-operations/>
	May 2018	During their previous campaign, we found Confucius using fake romance websites to entice victims into installing malicious Android applications. This time, the threat actor seems to have a new modus operandi, setting up two new websites and new payloads with which to compromise its targets. <https://blog.trendmicro.com/trendlabs-security-intelligence/confucius-update-new-tools-and-techniques-further-connections-with-patchwork/>
	Aug 2021	Confucius Uses Pegasus Spyware-related Lures to Target Pakistani Military <https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html>
Information	<https://unit42.paloaltonetworks.com/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/> <https://documents.trendmicro.com/assets/research-deciphering-confucius-cyberespionage-operations.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0142/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
