

Forum:[Hack Forums](#)

Thread: [Confucius Shifts from Document Stealers to Python Backdoors](#)

MadScientist - October 3, 2025, 5:17 am

A long-running cyber-espionage group known as Confucius has introduced new techniques in its campaigns against Microsoft Windows users.

First identified in 2013, the group has consistently targeted government agencies, defense contractors and critical industries across South Asia, particularly in Pakistan.

According to recent findings from FortiGuard Labs, what's new is Confucius' shift from document-focused stealers, such as WooperStealer, to more advanced Python-based backdoors like AnonDoor.

"This latest report from FortiGuard Labs highlights that threat actors are constantly adapting their techniques to stay ahead of the security research community, which develops new techniques to detect them," said John Bambenek, president at Bambenek Consulting.

"In particular, the use of Python tools exploits the persistent difficulty in detecting malicious activity within scripting languages, where you have a myriad of obfuscation techniques. Python is routinely used everywhere, which means attackers are free to leverage its power without having to install new tools or binaries as well."

FortiGuard researchers observed multiple attack chains between December 2024 and August 2025.

Early operations relied on spear-phishing with malicious Office documents and LNK files to deliver WooperStealer, a tool that exfiltrated a wide range of sensitive files, including documents, spreadsheets, images and emails.

By mid-2025, however, Confucius adopted a new approach. Instead of relying solely on data theft, the group began deploying the AnonDoor Python backdoor that provides long-term persistence and command execution capabilities. AnonDoor enables actions such as capturing screenshots, listing files, downloading data and dumping browser passwords.

Unlike previous campaigns that focused narrowly on document theft, AnonDoor is capable of full host profiling. It collects system details, geolocates public IPs and inventories disk volumes before receiving tasking from its command-and-control (C2) servers.

Researchers found that its operations were tailored toward targets in Pakistan, suggesting regionally focused objectives.

"This campaign underscores Confucius' technical agility," FortiGuard wrote, noting that the group can quickly pivot between different malware families and delivery methods to sustain access.

The report concludes that Confucius' layered attack chain demonstrates a clear evolution toward more durable, stealthy espionage operations.

Analysts caution that vigilance against such tactics remains crucial as state-linked groups continue to refine their methods.

Source - <https://www.infosecurity-magazine.com/news/confucius-shifts-doc-stealers/>