Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

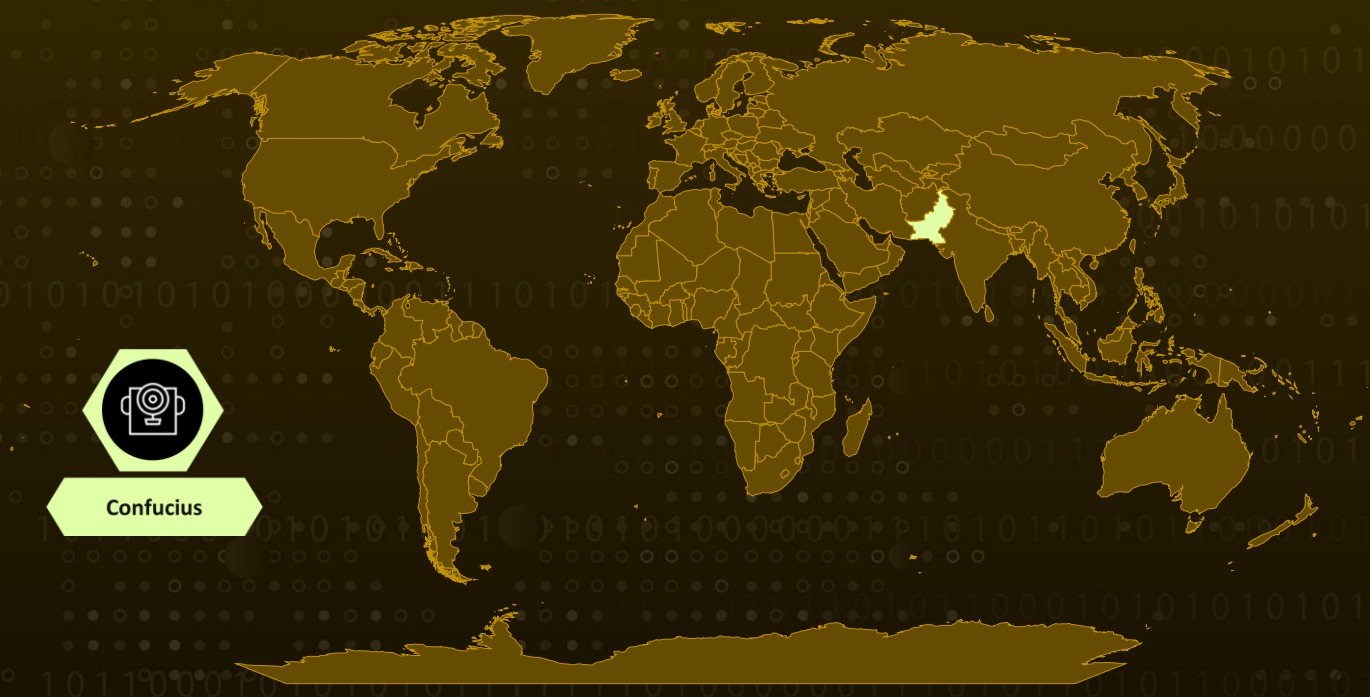
Confucius Hackers Spy on Critical Sectors Using AnonDoor

Date of Publication	Admiralty Code	TA Number
October 6, 2025	A1	TA2025305

Summary

Attack Commenced: August 2025
Malware: WooperStealer, AnonDoor
Threat Actor: Confucius (aka G0142)
Targeted Country: Pakistan
Targeted Industries: Government Agencies, Military Organizations, Defense Contractors, Critical Infrastructures
Affected Platform: Microsoft Windows
Attack: The Confucius group, an advanced South Asia-based cyber-espionage actor active since 2013, continues to evolve its operations by shifting from traditional stealers to sophisticated Python-based backdoors such as AnonDoor. Recent campaigns focus on maintaining long-term surveillance of high-value targets across government, defense, and other critical sectors.

Attack Regions



Attack Details

#1 The Confucius group, first identified in 2013, is a long-running cyber-espionage actor operating primarily across South Asia. It has repeatedly targeted government entities, military organizations, defense contractors, and other critical sectors, most prominently in Pakistan.

#2 Initial intrusions rely on targeted spear-phishing campaigns and malicious documents. Messages are crafted using authority spoofing, minimal contextual detail, and action-oriented prompts designed to persuade recipients to open attachments and initiate the infection chain. Victims are typically shown benign-looking decoy files while malicious payloads are deployed in the background.

#3 Early loaders use common system utilities to retrieve additional components. A recurring delivery technique involves a malicious shortcut .LNK files that execute a downloader Trojan to load further modules. DLL side-loading is frequently used to run rogue DLLs within otherwise legitimate binaries, enabling threat actors to evade detection.

#4 By late 2024 and into 2025, the Confucius group's tooling demonstrated a marked evolution. In December 2024, a campaign targeting Pakistan delivered the WooperStealer malware through a DLL side-loading lure. Follow-up activity in March 2025 employed LNK shortcuts to deploy the same stealer and facilitate data exfiltration. By August 2025, the threat actor leveraged a comparable LNK-based delivery chain to sideload a DLL that installed AnonDoor, a Python-based backdoor implant.

#5 AnonDoor functions as a persistent Python-based backdoor and a centralized loader for modular payloads. It supports long-term access and detailed host profiling by capturing screenshots and enumerating files and disk volumes. The toolset's componentized architecture enables streamlined deployment, flexible updates, and granular control over infected endpoints without altering core command-and-control pathways.

#6 Historically, the group relied on lightweight information stealers to harvest sensitive documents. The observable shift toward a distributed Python backdoor strategy signifies a move from short-term data theft toward establishing long-term remote access for sustained surveillance and follow-on operations.

Recommendations

Enhance Email Security and User Awareness: Implement advanced phishing filters to detect spear-phishing attempts and malicious attachments. Encourage verification of requests that appear to come from authoritative sources.

Segment Critical Networks and Limit Access: Implement strict network segmentation to isolate high-value assets. Apply least-privilege access controls and regularly review permissions to minimize potential lateral movement.

Implement Network Segmentation and Zero Trust Architecture: Segment networks to limit malware spread across interconnected systems. Apply zero trust principles, verify identity and device posture before granting access, regardless of location. Use micro-segmentation tools to define fine-grained access rules.

Regularly Review and Harden File System Permissions: Audit permissions for sensitive directories and ensure that only essential processes and users have write access. Disable file sharing where not required and use access control lists (ACLs) to limit exposure.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1204 User Execution	**T1204.002** Malicious File	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1059.006 Python	**T1053** Scheduled Task/Job	**T1053.005** Scheduled Task	**T1218** System Binary Proxy Execution

T1218.011 Rundll32	**T1082** System Information Discovery	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1574** Hijack Execution Flow	**T1574.001** DLL
T1041 Exfiltration Over C2 Channel	**T1112** Modify Registry	**T1005** Data from Local System	**T1083** File and Directory Discovery
T1087 Account Discovery	**T1113** Screen Capture	**T1027** Obfuscated Files or Information	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	marshmellowflowerscar[.]info, greenxeonsr[.]info, cornfieldblue[.]info, hauntedfishtree[.]info, petricgreen[.]info, bloomwpp[.]info, dropmicis[.]info, martkartout[.]info
SHA256	c91917ff2cc3b843cf9f65e5798cd2e668a93e09802daa50e55a842ba9e505de, 5a0dd2451a1661d12ab1e589124ff8ecd2c2ad55c8f35445ba9cf5e3215f977e, 4206ab93ac9781c8367d8675292193625573c2aaacf8feeaddd5b0cc9136d2d1, 8603b9fa8a6886861571fd8400d96a705eb6258821c6ebc679476d1b92dcd09e, 24b06b5caad5b09729ccaffa5a43352afd2da2c29c3675b17cae975b7d2a1e62,

TYPE	VALUE
SHA256	13ca36012dd66a7fa2f97d8a9577a7e71d8d41345ef65bf3d24ea5ebbb7c5ce1, 06b8f395fc6b4fda8d36482a4301a529c21c60c107cbe936e558aef9f56b84f6, 11391799ae242609304ef71b0efb571f11ac412488ba69d6efc54557447d022f, abefd29c85d69f35f3cf8f5e6a2be76834416cc43d87d1f6643470b359ed4b1b
URL	hxxps[:]//bloomwpp[.]info/hjdfyebvghu[.]pyc

References

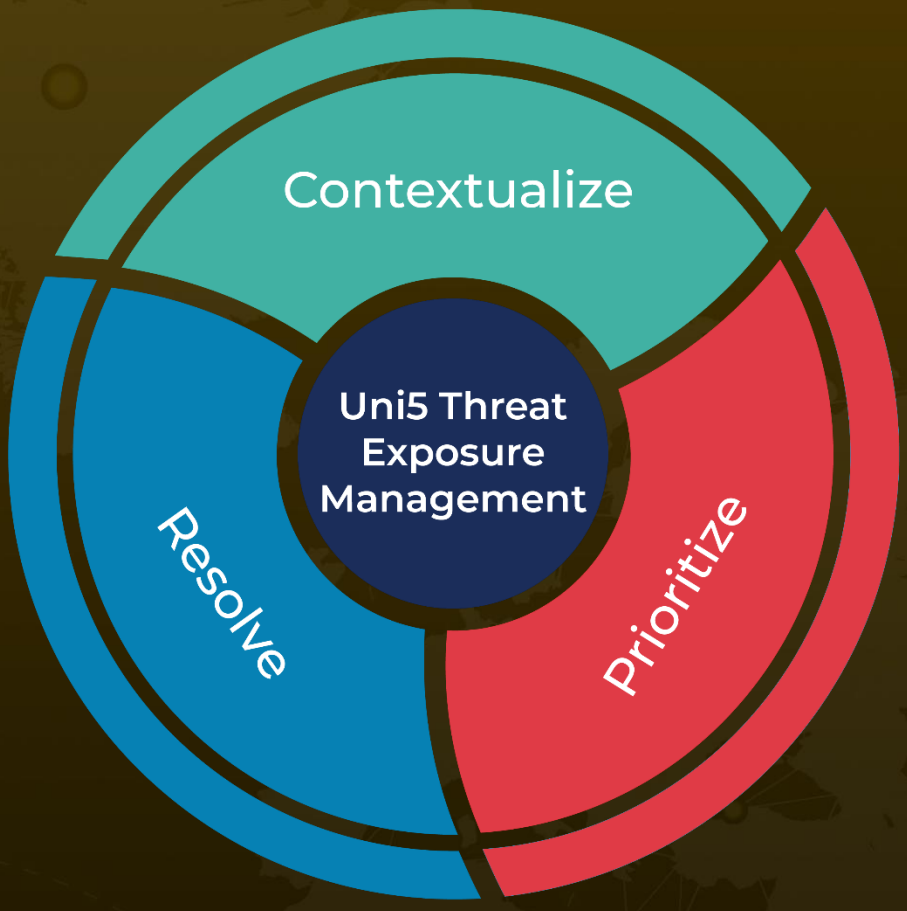
https://www.fortinet.com/blog/threat-research/confucius-espionage-from-stealer-to-backdoor

https://attack.mitre.org/groups/G0142/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 6, 2025 • 7:30 AM

More at www.hivepro.com