Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

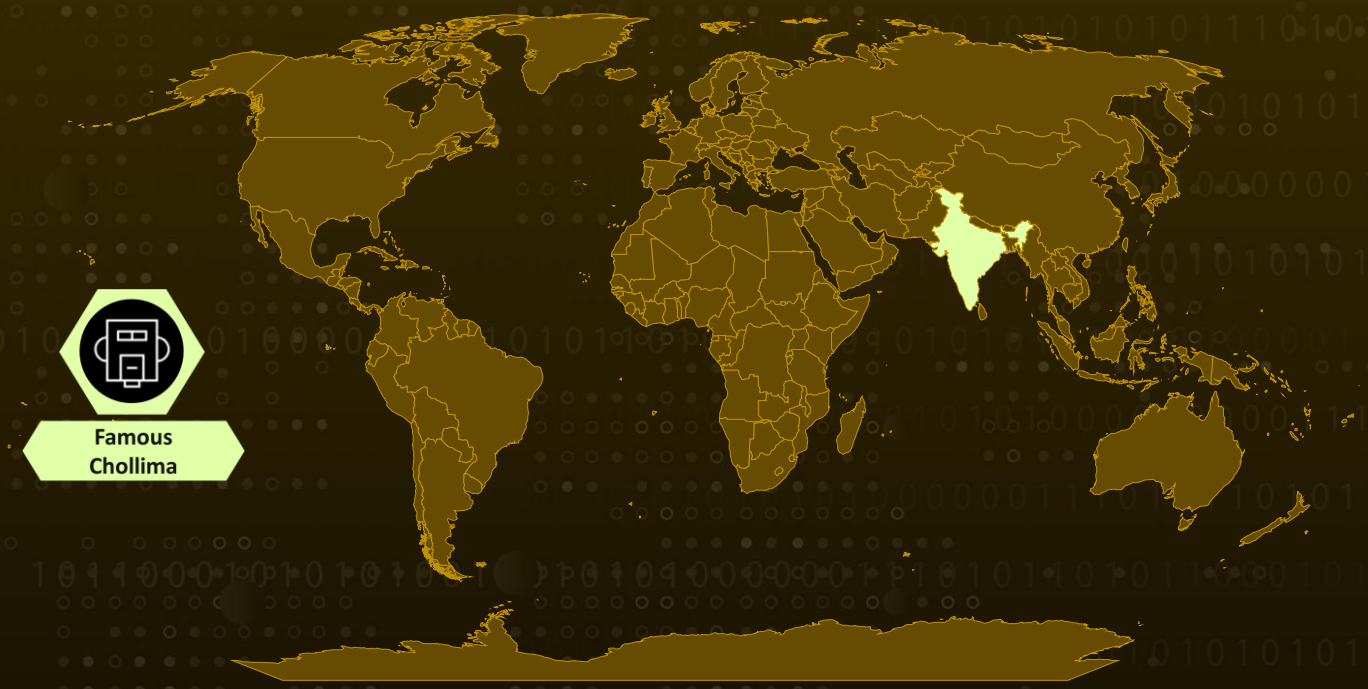
Famous Chollima Weaponizes Recruitment with PylangGhost RAT

Date of Publication	Admiralty Code	TA Number
June 20, 2025	A1	TA2025195

Summary

Attack Discovered: May 2025
Threat Actor: Famous Chollima (aka Wagemole, Contagious Interview, Nickel Tapestry, Storm-1877, UNC5267, Void Dokkaebi, PurpleBravo, TenaciousPungsan, WaterPlum, BadClone)
Malware: PylangGhost
Targeted Region: India
Targeted Industry: Cryptocurrency
Affected Platform: Windows
Attack: PylangGhost, a Python-based remote access trojan (RAT), has emerged as a weapon of choice for the North Korean-aligned group Famous Chollima, aimed at professionals pursuing careers in the cryptocurrency sector. This campaign demonstrates a dangerous blend of social engineering and technical sophistication, striking a fast-growing, high-value industry with precision.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 A Python-based remote access trojan (RAT) known as PylangGhost has been identified as an exclusive tool used by a North Korean-aligned group. PylangGhost mirrors the capabilities of the GolangGhost RAT, with each variant tailored for different operating systems: Python for Windows environments and Golang for macOS systems.

#2 The group behind these campaigns, tracked as Famous Chollima, pursues financial gain through a dual-faceted strategy. They pose as fictitious employers to lure job seekers into disclosing sensitive personal information and infiltrate targeted organizations by deploying fabricated employee profiles, securing insider access to corporate infrastructure.

#3 Their delivery method relies on elaborate social engineering operations disguised as legitimate job recruitment initiatives. These campaigns specifically target professionals in the cryptocurrency sector, with a primary focus on victims in India. The attackers impersonate well-known companies such as Coinbase, Robinhood, and Uniswap, creating deceptive skill assessment platforms built with React.

#4 Eventually, they are persuaded to execute malicious commands disguised as video driver installations, triggering the deployment of the RAT. The PylangGhost RAT functions through six coordinated Python modules that manage system compromise, data theft, and remote control. nvidia.py runs at system startup, creates registry entries, generates a unique GUID for command-and-control (C2) communications, and maintains a persistent command-response loop.

#5 The RAT enables remote system control, file manipulation, and credential theft from over 80 browser extensions, including cryptocurrency wallets and password managers. PylangGhost represents a technically proficient and highly targeted malware campaign that blends advanced coding with deceptive social engineering to steal credentials and sensitive information from individuals pursuing careers in the cryptocurrency industry.

Recommendations

Verify Recruiter Identities: Cross-check job offers and interview requests via official company channels or corporate emails. Avoid responding to unsolicited recruitment messages.

Maintain Multi-Factor Authentication (MFA): Enable MFA on all personal and professional accounts, including crypto exchange and wallet accounts, to reduce risks from credential theft.

Identify Social Engineering Red Flags: Recognize deceptive tactics like counterfeit video call interfaces, unexpected pop-ups, and prompts offering to "fix" audio or video problems. Emphasize avoiding clicks on unfamiliar or suspicious alerts during online meetings.

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
T1566 Phishing	**T1566.003** Spearphishing via Service	**T1189** Drive-by Compromise	**T1059** Command and Scripting Interpreter
T1059.006 Python	**T1204** User Execution	**T1204.004** Malicious Copy and Paste	**T1140** Deobfuscate/Decode Files or Information
T1036 Masquerading	**T1036.005** Match Legitimate Name or Location	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers
T1083 File and Directory Discovery	**T1012** Query Registry	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1027 Obfuscated Files or Information	**T1105** Ingress Tool Transfer	**T1113** Screen Capture	**T1560.001** Archive via Utility
T1560 Archive Collected Data	**T1543** Create or Modify System Process	**T1656** Impersonation	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	a206ea9b415a0eafd731b4eec762a5b5e8df8d9007e93046029d83316989790a, c2137cd870de0af6662f56c97d27b86004f47b866ab27190a97bde7518a9ac1b, 0d14960395a9d396d413c2160570116e835f8b3200033a0e4e150f5e50b68bec, 8ead05bb10e6ab0627fcb3dd5baa59cdaab79aa3522a38dad0b7f1bc0dada10a, 5273d68b3aef1f5ebf420b91d66a064e34c4d3495332fd492fecb7ef4b19624e, 267009d555f59e9bf5d82be8a046427f04a16d15c63d9c7ecca749b11d8c8fc3, 7ac3ffb78ae1d2d9b5d3d336d2a2409bd8f2f15f5fb371a1337dd487bd471e32, b7ab674c5ce421d9233577806343fc95602ba5385aa4624b42ebd3af6e97d3e5, fb5362c4540a3cbff8cb1c678c00cc39801dc38151edc4a953e66ade3e069225, d029be4142fca334af8fe0f5f467a0e0e1c89d3b881833ee53c1e804dc912cfd, b8402db19371db55eebea08cf1c1af984c3786d03ff7eae954de98a5c1186cee, 1f482ce7e736a8541cc16e3e80c7890d13fb1f561ae38215a98a75dce1333cee, ed170975e3fd03440360628f447110e016f176a44f951fcf6bc8cdb47fbd8e0e, 929c69827cd2b03e7b03f9a53c08268ab37c29ac4bd1b23425f66a62ad74a13b, 127406b838228c39b368faa9d6903e7e712105b5ad8f43a987a99f7b10c29780, 0ec9d355f482a292990055a9074fdabdb75d72630b920a61bdf387f2826f5385, c2d2320ae43aaa0798cbcec163a0265cba511f8d42d90d45cd49a43fe1c40be6, e7c2b524f5cb0761a973accc9a4163294d678f5ce6aca73a94d4e106f4c8fea4, 28198494f0ed5033085615a57573e3d748af19e4bd6ea215893ebeacf6e576df, fc71a1df2bb4ac2a1cc3f306c3bdf0d754b9fab6d1ac78e4eceba5c6e7aee85d, d3500266325555c9e777a4c585afc05dfd73b4cbe9dba741c5876593b78059fd

TYPE	VALUE
URLs	hxxp[:]//31[.]57[.]243[.]29[:]8080, hxxp[:]//154[.]58[.]204[.]15[:]8080, hxxp[:]//212[.]81[.]47[.]217[:]8080, hxxp[:]// 31[.]57[.]243[.]190[:]8080
Hostname	api[.]quickcamfix[.]online, api[.]auto-fixer[.]online, api[.]quickdriverupdate[.]online, api[.]camtuneup[.]online, api[.]driversofthub[.]online, api[.]drive-release[.]cloud, api[.]vcamfixer[.]online, api[.]nvidia-drive[.]cloud, api[.]nvidia-release[.]us, api[.]autodriverfix[.]online, api[.]camdriversupport[.]com, api[.]smartdriverfix[.]cloud, api[.]drivercams[.]cloud, api[.]camtechdrivers[.]com, api[.]web-cam[.]cloud, api[.]camera-drive[.]org, api[.]nvidia-release[.]org, api[.]fixdiskpro[.]online, api[.]autocamfixer[.]online
Domains	krakenhire[.]com, yuga[.]skillquestions[.]com, uniswap[.]speakure[.]com, doodles[.]skillquestions[.]com, www[.]hireviavideo[.]com, kraken[.]livehiringpro[.]com, quiz-nest[.]com, www[.]smartvideohire[.]com, www[.]talent-hiringstep[.]com, provevidskillcheck[.]com, skill[.]vidintermaster[.]com, digitaltalent[.]review, robinhood[.]ecareerscan[.]com, evalswift[.]com, livetalentpro[.]com, quantumnodespro[.]com, evalassesso[.]com, parallel[.]eskillora[.]com, coinbase[.]talentmonitoringtool[.]com, uniswap[.]testforhire[.]com, coinbase[.]talenthiringtool[.]com, crosstheages[.]skillence360[.]com,

TYPE	VALUE
Domains	assesstrack[.]com, talent-hiringtalk[.]com, uniswap[.]prehireiq[.]com, fast-video-recording[.]com, parallel[.]eskillprov[.]com,
Filename	nvidia.py

References

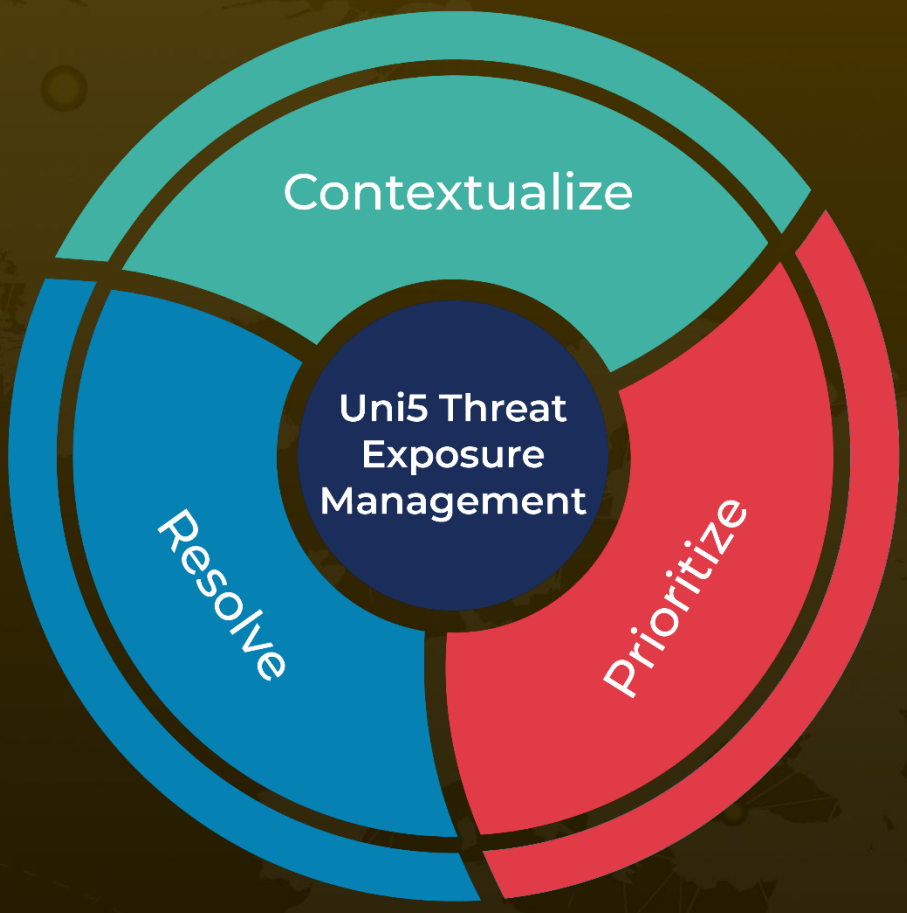
https://blog.talosintelligence.com/python-version-of-golangghost-rat/

https://hivepro.com/threat-advisory/clickfake-interview-lazarus-groups-new-crypto-heist-via-fake-job-offers/

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

June 20, 2025 • 1:00 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com