Famous Chollima’s PylangGhost

blog.polyswarm.io/famous-chollimas-pylangghost

Verticals Targeted: Cryptocurrency
Regions Targeted: India
Related Families: GolangGhost

Executive Summary

Famous Chollima, a North Korean-aligned threat actor, has deployed PylangGhost, a Python-based remote access trojan (RAT), targeting cryptocurrency and blockchain professionals in India. This malware, a variant of the GolangGhost RAT, facilitates credential theft and remote system control via sophisticated social engineering tactics.

Key Takeaways

- PylangGhost, a Python-based RAT, mirrors the functionality of the GolangGhost RAT, targeting Windows systems in cryptocurrency and blockchain sectors.
- The malware is delivered through fake job recruitment platforms, leveraging social engineering to trick victims into executing malicious scripts.
- PylangGhost steals credentials from over 80 browser extensions, including cryptocurrency wallets and password managers.

What is PylangGhost?

In May 2025, Cisco Talos identified PylangGhost, a Python-based remote access trojan (RAT) deployed by the North Korean-aligned threat actor Famous Chollima. This malware targets Windows systems, while its predecessor, the Golang-based GolangGhost RAT, continues to target macOS users. PylangGhost is delivered through a sophisticated social engineering campaign aimed at professionals in the cryptocurrency and blockchain industries, primarily in India. The campaign exploits jobseekers by posing as recruiters from reputable companies, such as Coinbase and Robinhood, to lure victims into executing malicious code.

The infection chain begins when victims are directed to fake job application websites that instruct them to copy and execute a command line, typically using PowerShell Invoke-WebRequest or curl. This command downloads a ZIP file containing PylangGhost's six Python modules, a Visual Basic Script (VBS), and a renamed Python interpreter disguised as "nvidia.py." The VBS unzips a Python library ("lib.zip") and launches the RAT by executing the interpreter with "nvidia.py" as the main program. This script establishes persistence by creating a registry value to ensure the RAT runs at system login, generates a unique system GUID for command-and-control (C2) communication, and enters a command loop using RC4-encrypted HTTP packets to interact with the C2 server.

PylangGhost's functionality is nearly identical to GolangGhost, enabling remote system control, file manipulation, and credential theft from over 80 browser extensions, including cryptocurrency wallets like MetaMask, Phantom, and TronLink, as well as password managers such as 1Password and NordPass. The Python modules are well-structured, and

their naming conventions and architecture closely resemble those of the Golang variant, suggesting a unified development team. The configuration file “config.py” defines commands identical to those in GolangGhost, facilitating consistent malicious operations across both variants.

The campaign’s focus on cryptocurrency and blockchain professionals underscores Famous Chollima’s financial motivations, likely aiming to steal sensitive credentials and assets. Open-source intelligence indicates a limited impact, with a small number of affected users predominantly in India, suggesting a targeted rather than widespread campaign. The use of Python for Windows and Golang for macOS may reflect strategic choices to optimize platform-specific delivery or evade detection, though the rationale for dual variants remains unclear. The close alignment between PylangGhost and GolangGhost highlights Famous Chollima’s evolving tactics.

Who is Famous Chollima?

Famous Chollima, also known as Wagemole, Nickel Tapestry, Purple Bravo, Tenacious Pungsan, Void Dokkaebi, Storm-1877, and UNC5267 is a North Korea nexus threat actor active since at least 2018. Their activities primarily focus on financial gain and espionage to support the DPRK regime. The group is assessed to be affiliated with North Korea’s Reconnaissance General Bureau, a key intelligence service.

Famous Chollima employs sophisticated social engineering, posing as legitimate remote IT workers to infiltrate organizations. They create fraudulent identities, falsify resumes, and use generative AI to craft convincing profiles, securing roles at small to mid-sized businesses via platforms like Upwork and LinkedIn. Once embedded, they deploy custom malware, such as BeaverTail and InvisibleFerret, to steal credentials and sensitive data. The group leverages fake job recruitment campaigns, delivering malicious Python-based RATs like PylangGhost to target cryptocurrency and blockchain sectors. They establish persistence through registry modifications and use RC4-encrypted HTTP for command-and-control communication.

Famous Chollima targets cryptocurrency, blockchain, and technology sectors, with a notable focus on India and Western countries, including the US, Germany, and Ukraine. Their operations fund North Korea’s regime through illicitly earned salaries and stolen assets, evading international sanctions. The group’s infrastructure often relies on anonymization networks to conceal their activities.

IOCs

PolySwarm has a sample associated with this activity.

c2137cd870de0af6662f56c97d27b86004f47b866ab27190a97bde7518a9ac1b

You can use the following CLI command to search for all PylangGhost samples in our portal:

$ polyswarm link list -f PylangGhost

Don't have a PolySwarm account? Go here to sign up for a free Community plan or subscribe.

Contact us at hivemind@polyswarm.io | Check out our blog | Subscribe to our reports.

Topics: Blockchain, Threat Bulletin, North Korea, India, Malware, Python, Cryptocurrency, RAT, PylangGhost, GolangGhost, Famous Chollima

Written by The Hivemind