# New Python backdoor signals a shift in ransomware tactics



A newly identified Python-based backdoor, suspected to be developed with the assistance of artificial intelligence, has emerged as a critical instrument for affiliates of RansomHub, a relatively new player in the ransomware landscape. This backdoor allows cybercriminals to infiltrate and maintain access to compromised networks, according to Andrew Nelson, Principal Digital Forensics and Incident Response Consultant at GuidePoint Security. The findings, which represent a significant shift in tactics employed by ransomware groups, were discussed in a report by Information Security Buzz.

RansomHub, introduced to the cybercrime scene in February 2024, has made a name for itself as a Ransomware-as-a-Service (RaaS) operation. The group has garnered attention not only for its efficacy but also for its affiliate payment model, which is notably generous at a 90/10 split. Affiliates retain 90% of ransom payments, which is substantially higher than what is typically seen among competing ransomware groups. This model, paired with the group’s technological capabilities—supporting various operating systems including Windows, Linux, and ESXi—positions RansomHub as a formidable threat to global businesses.

The sophistication of the backdoor utilised by RansomHub affiliates is evident in its deployment method. It is installed via Remote Desktop Protocol (RDP), allowing intruders to embed themselves within a target network. Once in position, they can deploy ransomware encryptors across locked-down systems with relative ease. The tool’s design is intricate, employing heavy obfuscation practices sourced from services like PyObfuscate to elude detection efforts by cybersecurity professionals.

GuidePoint Security’s evaluation of the backdoor has uncovered unique indicators of compromise, such as:

* Obfuscated task and filename nomenclature,
* Command-and-control (C2) address patterns, and
* An innovative use of the SOCKS5 protocol, which enables persistent connections for seamless lateral movement within infected networks.

The profound quality of the backdoor's code suggests that AI might have played a role in its development. According to Nelson, "the Python code is structured with clearly defined classes, descriptive variable names, and comprehensive error handling," which are hallmarks of AI-assisted programming. Even amidst obfuscation, the code remains accessible for further analysis if de-obfuscated, revealing the skill and resources behind its creation.

The elaborate attack lifecycle initiated by these affiliates begins with the deployment of SocGholish (FakeUpdate) malware, aimed at securing initial access. Upon breaching the target, the actors can deploy the Python backdoor swiftly, signalling a capability to escalate privileges and execute lateral movements across the network within moments. Significant components of the deployment process encompass the installation of Python and requisite libraries, configuring a reverse proxy script, and establishing persistence through scheduled tasks within Windows.

Recent enhancements to the Python backdoor reveal ongoing updates that include:

* Hardcoded C2 variables to strengthen operation stealth,
* Improved obfuscation measures to evade detection,
* A refined tunnelling mechanism for TCP traffic, limited, however, to IPv4, excluding IPv6 compatibility.

In conducting their analysis, GuidePoint Security discovered 18 active IP addresses linked to this C2 framework, which they have shared through a collaborative GitHub feed for broader community engagement.

The emergence of this advanced tool underscores the evolving landscape of ransomware operations, particularly with regards to how groups, such as RansomHub, increasingly harness AI and advanced coding techniques to refine their malicious capabilities. This trend poses rising concerns for businesses that must now look towards enhanced defensive measures, which include vigilant monitoring for concealed scripts, comprehensive employee training programs to thwart social engineering attempts, and the proactive use of threat intelligence feeds to stay ahead of identified compromise indicators.

As the threat posed by RansomHub solidifies, the combination of AI-driven progress and sophisticated malware tactics highlights an urgent necessity for businesses to adapt and fortify their cybersecurity strategies. The findings presented by GuidePoint Security shed light on the pressing nature of this threat, emphasising the importance of real-time intelligence and adaptive defensive measures in navigating this increasingly perilous environment.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://informationsecuritybuzz.com/ransomhub-exploit-ai-generated-python/> - Corroborates the identification of a Python-based backdoor developed with AI assistance, its deployment via RDP, and its use by RansomHub affiliates.
2. <https://informationsecuritybuzz.com/ransomhub-exploit-ai-generated-python/> - Details RansomHub's introduction to the cybercrime scene in February 2024, its RaaS model, and the generous 90/10 affiliate payment split.
3. <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub> - Provides information on RansomHub's targeting of larger enterprises, its use of ransomware variants in GoLang and C++, and its affiliate recruitment through the RAMP forum.
4. <https://informationsecuritybuzz.com/ransomhub-exploit-ai-generated-python/> - Explains the sophistication of the backdoor, including its deployment via RDP, heavy obfuscation, and use of the SOCKS5 protocol for lateral movement.
5. <https://www.guidepointsecurity.com/blog/ransomhub-affiliate-leverage-python-based-backdoor/> - Supports the unique indicators of compromise such as obfuscated filenames, C2 addresses, and the use of the SOCKS5 protocol.
6. <https://informationsecuritybuzz.com/ransomhub-exploit-ai-generated-python/> - Discusses the quality of the backdoor's code, suggesting AI involvement due to its structured classes, descriptive variable names, and comprehensive error handling.
7. <https://www.guidepointsecurity.com/blog/ransomhub-affiliate-leverage-python-based-backdoor/> - Details the attack lifecycle, including the initial access via SocGholish malware, deployment of the Python backdoor, and establishment of persistence through scheduled tasks.
8. <https://informationsecuritybuzz.com/ransomhub-exploit-ai-generated-python/> - Highlights recent enhancements to the Python backdoor, including hardcoded C2 variables, improved obfuscation, and a refined tunnelling mechanism for TCP traffic.
9. <https://www.guidepointsecurity.com/blog/ransomhub-affiliate-leverage-python-based-backdoor/> - Mentions the discovery of 18 active IP addresses linked to the C2 framework and their sharing through a collaborative GitHub feed.
10. <https://informationsecuritybuzz.com/ransomhub-exploit-ai-generated-python/> - Emphasizes the evolving landscape of ransomware operations, particularly the use of AI and advanced coding techniques by groups like RansomHub.
11. <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub> - Underlines the need for enhanced defensive measures, including continuous monitoring, employee training, and the use of threat intelligence feeds to counter RansomHub's threats.
12. <https://informationsecuritybuzz.com/ransomhub-exploit-ai-generated-python/> - Please view link - unable to able to access data