Python Malware: How Cybercriminals Use It in 2025

Cybercrime isn’t what it used to be. In 2025, the code driving many cyber attacks is written in Python—a language that once thrived solely in academic circles and data science communities.

Today, Python’s clean syntax, robust libraries, and sheer versatility have made it the top scripting language for both cybercriminals and cybersecurity experts alike.

In this article, we’re going to break down how Python malware has evolved, how artificial intelligence (AI) is both defending against and enhancing cyber attacks, and how ethical hackers use Python for red team operations.

Expect practical advice, code examples, and real-world stats that you can put to work immediately.

1. The Evolution of Python Malware

From Simple Scripts to Sophisticated Threats

Python started as a tool for developers seeking readability and simplicity. Over the years, these very qualities have turned Python into a double-edged sword.

Cybercriminals favor Python for creating malware because it’s easy to write, modify, and deploy across multiple platforms.

What began as rudimentary scripts for stealing data has evolved into sophisticated tools such as Remote Access Trojans (RATs), ransomware, and keyloggers.

Info: "Python’s accessibility means that both amateurs and professionals can craft powerful malware in just a few lines of code."

**Remote Access Trojans (RATs):**

RATs allow attackers to control a victim’s system remotely. Modern Python-based RATs can bypass traditional security measures.

They use obfuscation techniques and dynamic code loading to hide their presence.

For example, a basic Python RAT might use the built-in socket module to open a command shell on a target machine:

Texto

O conteúdo gerado por IA pode estar incorreto.

https://dev.to/snappytuts/python-malware-how-cybercriminals-use-it-in-2025-3e8m?fbclid=IwY2xjawJG\_x1leHRuA2FlbQIxMQABHYwe8UIO\_UZldjs8shOpwSrjfudkLufBE6DLY5DX8Q2HFLqHCRhr1aVrKg\_aem\_KhE7JWGV2\_poyMXhFLbfKA