Who: [United Nations Development Program (UNDP)](https://www.bleepingcomputer.com/news/security/united-nations-agency-investigates-ransomware-attack-claimed-by-8Base-gang/)

What: The perpetrators utilized a custom version of Phobos. [Phobos](https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a) uses a three-phase deployment. 1st, Smokeloader manipulates either VirtualAlloc or VirtualProtect API functions to open an entry point, which enables code to be injected into running processes. 2nd, a stealth process is used to obfuscate command and control activity by producing requests to legitimate websites. In addition, during this phase a portable executable is prepared for deployment. And finally, a program-erase cycle is unpacked from stored memory, which is then extracted from a SHA256 hash as a payload. Once the payload is decrypted, additional malware is downloaded.

Who: 8base, a potential offshoot of RansomHouse.

Payment: It does not appear so, [a spokesperson from the UNDP stated that they “do not engage with threat actors” and that “no ransom has or will be paid.”](https://www.blackfog.com/the-state-of-ransomware-2024/)