A New Breed of Spyware Quietly Watches Through Your Camera

September 18, 2025 - Thereâ€™s a new kind of digital pickpocket prowling the internet, and it isnâ€™t just after your passwords
Called Stealerium, this open-source spyware has security experts worried not only because of what it can steal, but how it might be used to humiliate or blackmail people in deeply personal ways. Researchers at Proofpoint, a well-known cybersecurity firm, recently reported that Stealerium includes an unusual feature: it can watch for adult content in your web browser and, if it spots something, quietly snap screenshots and even activate your webcam to capture your reaction. Itâ€™s the kind of tool that could turn private moments into leverage for extortion.
So far, there are no confirmed cases of anyone actually being blackmailed using Stealerium. But the potential is clear, and history shows that itâ€™s not far-fetched. A decade ago, a former classmate of Miss Teen USA Cassidy Wolf used different spyware to secretly take photos through her webcam and tried to extort her for more. And back in 2019, another piece of malware called Varenyky was caught spying on French users while they viewed pornography, then threatening to release the footage unless they paid up. Stealerium hasnâ€™t been linked to a case like that yetâ€”but it has all the necessary tools built in.

Even if blackmail isnâ€™t the goal, Stealerium still poses serious risks. Like other â€œinfostealerâ€• malware, itâ€™s designed rummage through a computer and quietly pull out whatever it can find: saved passwords, cookies, browser history, documents, Wi-Fi credentials, and screenshots of whateverâ€™s on your screen. That sort of data can fuel identity theft, account takeovers, and financial fraud long after the infection is gone. Itâ€™s the digital equivalent of someone copying every key on your keyring before you notice they were even in the room.

What makes this more concerning is how easily it spreads. Most infections start with phishing emails carrying booby-trapped attachmentsâ€”usually ZIP or ISO files pretending to be invoices, resumes, or security notices. Other campaigns hide the malware inside fake software downloads or cracked programs, often promoted through malicious ads or search-engine tricks. Some even circulate on messaging platforms like Discord and Telegram, disguised as tools or game mods. In every case, it depends on someone being persuaded to click and run it. Once launched, it can install itself silently, disable antivirus tools, and begin exfiltrating data within minutes.

Adding to the unease is how Stealerium first surfaced. It was released on GitHub as open-source softwareâ€”freely available for anyone to downloadâ€”with the claim that it was â€œfor educational purposes only.â€• That disclaimer offers little comfort, si open-source malware often ends up repurposed by criminals. Proofpointâ€™s analysts have already seen multiple threat groups adapt Stealerium into their own campaigns. Like many open-source attack tools, what may have begun as a programming showcase or security research project is now being used against unsuspecting people.

Stealerium isnâ€™t alone. Other stealers like RedLine, Raccoon, and Vidar have infected millions of computers worldwide in recent years, siphoning off credentials and personal data. But Stealeriumâ€™s voyeuristic twist makes it stand outâ€”and not in a good way. Itâ€™s a reminder that our personal devices are not just windows into the world, but windows the world can sometimes peer back through.

For most people, defending against this kind of threat starts with simple caution. Be skeptical of unexpected attachments, resist the temptation of â€œfreeâ€• cracked software, and keep security updates turned on. Covering your webcam isnâ€™t paranoia; itâ€™s just common sense. Tools like Stealerium may have been built under the banner of education, but theyâ€™ve clearly graduated into something else entirely.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS