# XWorm malware resurfaces with ransomware module, over 35 plugins

XWorm malware resurfaces with ransomware module, over 35 plugins By Ionut Ilascu October 6, 2025 07:42 AM New versions of the XWorm backdoor are being distributed in phishing campaigns after the original developer, XCoder, abandoned the project last year. The latest variants, XWorm 6.0, 6.4, and 6.5, appear to be adopted by multiple threat actors and have support for plugins that allow a wide range of malicious activities. Malware operators can use the modules to steal data from browsers and applications, take control of the host through remote desktop and shell access, and encrypt or decrypt files. The last known version of the malware developed by XCoder is 5.6, which was vulnerable to a remote code execution flaw, addressed in the recent variants. Versatile and popular XWorm is a remote access trojan first observed in 2022. It gained a reputation as a highly effective malware due to its modular architecture and extensive capabilities. It is typically used to collect sensitive data (passwords, crypto wallets, financial info), track keystrokes, steal information in the clipboard, However, it can also be used to launch distributed denial-of-service (DDoS) attacks and load other malware. After XCoder deleted their Telegram accounts, where they shared regular updates, multiple threat actors started to spread cracked versions of the malware. XWorm was so popular that a threat actor used it as a lure to target less-skilled cybercriminals with a backdoor that stole data. That campaign counted 18,459 infections , most of them in Russia, the United States, India, Ukraine, and Turkey. Variety of delivery methods Since June, researchers at cybersecurity company Trellix have noticed an increase in XWorm samples on the VirusTotal scanning platform, which also indicates a high adoption rate among cybercriminals. In one phishing campaign, the malware was deployed through a malicious JavaScript that initiated a PowerShell script, which could bypass the Antimalware Scan Interface protection and deploy XWorm. XWorm infection chain source: Trellix In a report from September, the researchers said that the XWorm malware infection chain has evolved to include additional techniques beyond traditional email-based attacks. Email and .LNK files are still a common initial access vector, but the malware also uses legitimate-looking .exe filenames to disguise itself as harmless applications such as Discord. This marks a shift towards combining social engineering with technical attack vectors for greater effectiveness, Trellix said . Other researchers detected campaigns that delivered XWorm using AI-themed lures and a modified variant of the ScreenConnect remote access tool. Another research provides technical details on an phishing campaign delivering XWorm through shellcode embedded in a Microsoft Excel file (.XLAM).

Ransomware threat among dozens of modules According to Trellix researchers, XWorm now has more than 35 plugins that extend its capabilities from stealing sensitive information to ransomware. The file encrypting functionality, Ransomware.dll, lets malware operators set a desktop wallpaper after locking the data, the ransom amount, wallet address, and contact email. Options for XWorm operator launching a ransomware attack source: Trellix The encryption process avoids system files and folders and focuses on data in the %USERPROFILE% and Documents locations, deletes the original file, and adds the .ENC extension to the locked data. Victims also get instructions to decrypt the data in an HTML file dropped on the desktop. Details include the BTC address, email ID, and ransom amount. XWorm ransomware module encryption source: Trellix Trellix researchers found code overlaps between XWorm s ransomware module and the .NET-based NoCry ransomware first observed in 2021. Both pieces of malicious code use the same algorithm to generate the initialization vector (IV) and the encryption/decryption key, the encryption process (AES with CBC mode in blocks of 4096 bytes). The researchers also noticed that the two pieces of malware ran the same set of verifications against analysis environments. Apart from the ransomware component, Trellix analyzed 14 other plugins for XWorm: RemoteDesktop.dll : creates a remote session to interact with the victim s machine WindowsUpdate.dll , Stealer.dll , Recovery.dll , merged.dll , Chromium.dll , and SystemCheck.Merged.dll : steal victims' data FileManager.dll : provides the operator filesystem access and manipulation capabilities Shell.dll : executes system commands the operator sends in a hidden cmd.exe process Informations.dll : gathers system information about the victim's machine Webcam.dll : Used to record the victim. It is also used by the operator to verify if an infected machine is real TCPConnections.dll , ActiveWindows.dll , and StartupManager.dll : send a list of active TCP connections, active windows, and startup programs, respectively, to the C2 server The researchers say that the data theft modules alone allow an XWorm operator to steal login data from multiple applications that include more than 35 web browsers, email clients, messaging apps, FTP clients, and crypto wallets. Since plugins serve a specific function, Trellix recommends that organizations use a multi-layered defense approach that can respond to malicious activity after compromise. Endpoint detection and response (EDR) solutions can identify the behavior of XWorm s modules, while proactive email and web protections can block the initial malware droppers. Additionally, a network monitoring solution could detect the communication with the command and control server for downloading more plugins or data exfiltration.