# Lazarus Group Exploits Zero-Day Vulnerability to Hack South Korean Financial Entity

By The Hacker News

Published: 2023-03-08 · Archived: 2026-04-05 19:39:37 UTC

The North Korea-linked **Lazarus Group** has been observed weaponizing flaws in an undisclosed software to breach a financial business entity in South Korea twice within a span of a year.

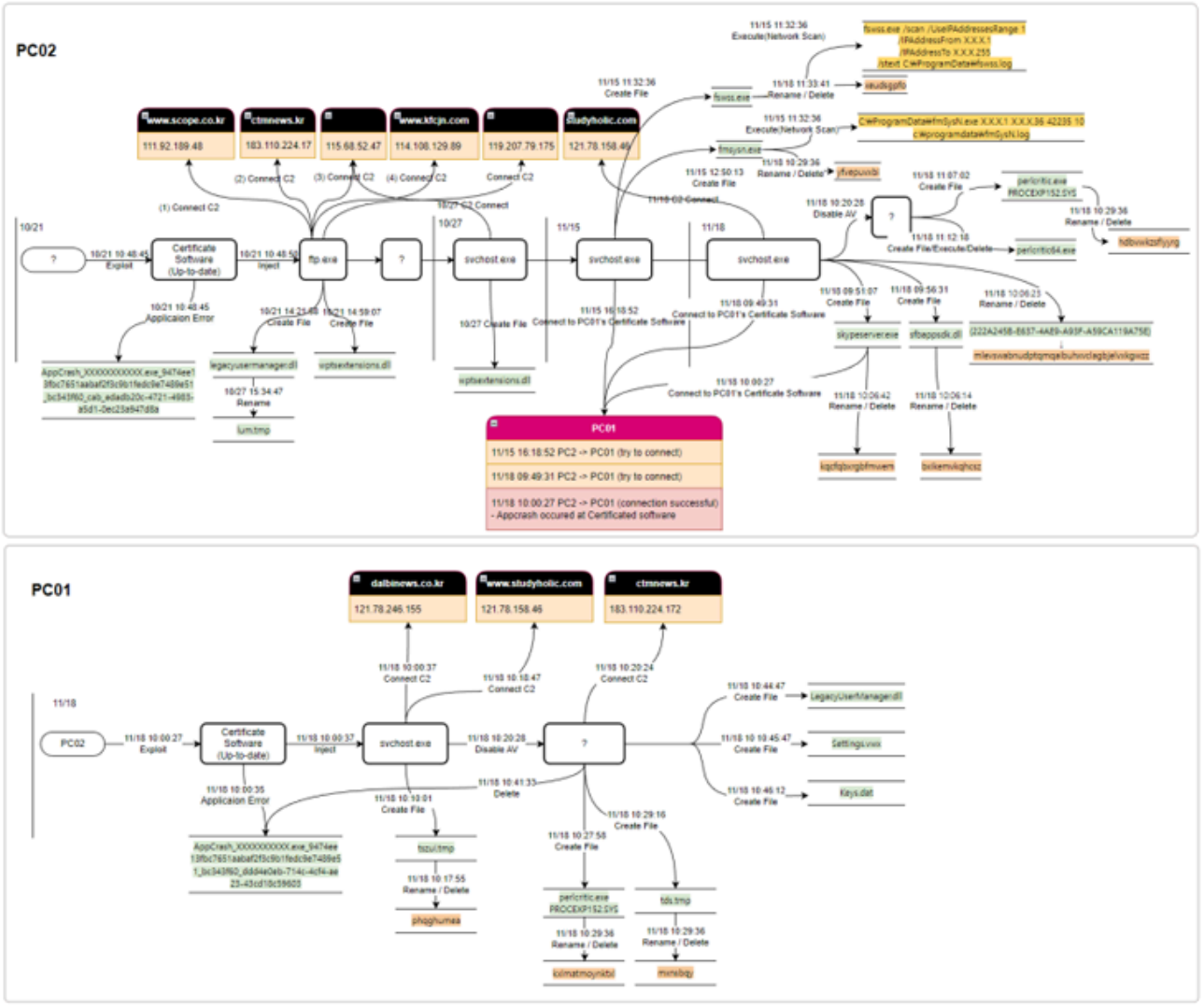
While the first attack in May 2022 entailed the use of a vulnerable version of a certificate software that's widely used by public institutions and universities, the re-infiltration in October 2022 involved the exploitation of a zero-day in the same program.

Cybersecurity firm AhnLab Security Emergency Response Center (ASEC) said it's refraining from divulging more specifics owing to the fact that "the vulnerability has not been fully verified yet and a software patch has not been released."

The adversarial collective, after obtaining an initial foothold by an unknown method, abused the zero-day bug to perform lateral movement, shortly after which the AhnLab V3 anti-malware engine was disabled via a BYOVD attack.



It's worth noting here that the Bring Your Own Vulnerable Driver, aka BYOVD, technique has been repeatedly employed by the Lazarus Group in recent months, as documented by both ESET and AhnLab in a series of reports late last year.




Among other steps taken to conceal its malicious behavior include changing file names before deleting them and modifying timestamps using an anti-forensic technique referred to as timestomping.

The attack ultimately paved the way for multiple backdoor payloads (Keys.dat and Settings.vwx) that are designed to connect to a remote command-and-control (C2) server and retrieve additional binaries and execute them in a fileless manner.



The development comes a week after ESET shed light on a new implant called WinorDLL64 that's deployed by the notorious threat actor by means of a malware loader named Wslink.

"The Lazarus Group is researching the vulnerabilities of various other software and are constantly changing their TTPs by altering the way they disable security products and carry out anti-forensic techniques to interfere or delay detection and analysis in order to infiltrate Korean institutions and companies," ASEC said.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

---