

# Rclone, Software S1040 | MITRE ATT&CK®

Archived: 2026-04-05 15:44:12 UTC

[Rclone](#) is a command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA. [Rclone](#) has been used in a number of ransomware campaigns, including those associated with the [Conti](#) and DarkSide Ransomware-as-a-Service operations. [\[1\]\[2\]\[3\]\[4\]\[5\]](#)



Platforms: Linux, Windows, macOS

Contributors: Edward Millington; Ian McKay

Last Modified: 14 October 2025

## Techniques Used

## Groups That Use This Software

## Campaigns

## References

1. [Nick Craig-Wood. \(n.d.\). Rclone syncs your files to cloud storage. Retrieved August 30, 2022.](#)
2. [Justin Schoenfeld and Aaron Didier. \(2021, May 4\). Rclone Wars: Transferring leverage in a ransomware attack. Retrieved August 30, 2022.](#)
3. [Aaron Greetham. \(2021, May 27\). Detecting Rclone – An Effective Tool for Exfiltration. Retrieved August 30, 2022.](#)
4. [Ramarcus Baylor. \(2021, May 12\). DarkSide Ransomware Gang: An Overview. Retrieved August 30, 2022.](#)
5. [DFIR Report. \(2021, November 29\). CONTInuing the Bazar Ransomware Story. Retrieved September 29, 2022.](#)
6. [Mandiant Incident Response. \(2025, May 6\). Defending Against UNC3944: Cybercrime Hardening Guidance from the Frontlines. Retrieved October 13, 2025.](#)
7. [Cybersecurity and Infrastructure Security Agency. \(2025, March 12\). AA25-071A #StopRansomware: Medusa Ransomware. Retrieved October 15, 2025.](#)
8. [Threat Hunter Team Symantec and Carbon Black. \(2025, March 6\). Medusa Ransomware Activity Continues to Increase. Retrieved October 15, 2025.](#)
9. [Microsoft Threat Intelligence. \(2024, September 26\). Storm-0501: Ransomware attacks expanding to hybrid cloud environments. Retrieved October 19, 2025.](#)
10. [Carvey, H. \(2024, May 1\). LOLBin to INC Ransomware. Retrieved June 5, 2024.](#)

11. [US Cybersecurity & Infrastructure Security Agency et al. \(2024, September 5\). Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure. Retrieved September 6, 2024.](#)
12. [Steven Campbell, Akshay Suthar, & Connor Belfiorre. \(2023, July 26\). Conti and Akira: Chained Together. Retrieved February 20, 2024.](#)
13. [Biderman, O. et al. \(2022, October 3\). REVEALING EMPEROR DRAGONFLY: NIGHT SKY AND CHEERSCRYPT - A SINGLE RANSOMWARE GROUP. Retrieved December 6, 2023.](#)

---

Source: <https://attack.mitre.org/software/S1040>