



Written for

This section shows the list of targeted audiences that the article is written for

[Skip to main content](#)

- [ABOUT NCSC](#)
- [CISP](#)
- [REPORT AN INCIDENT](#)
- [CONTACT US](#)

- [Home](#)

report

[Download / Print article PDF](#)

Share



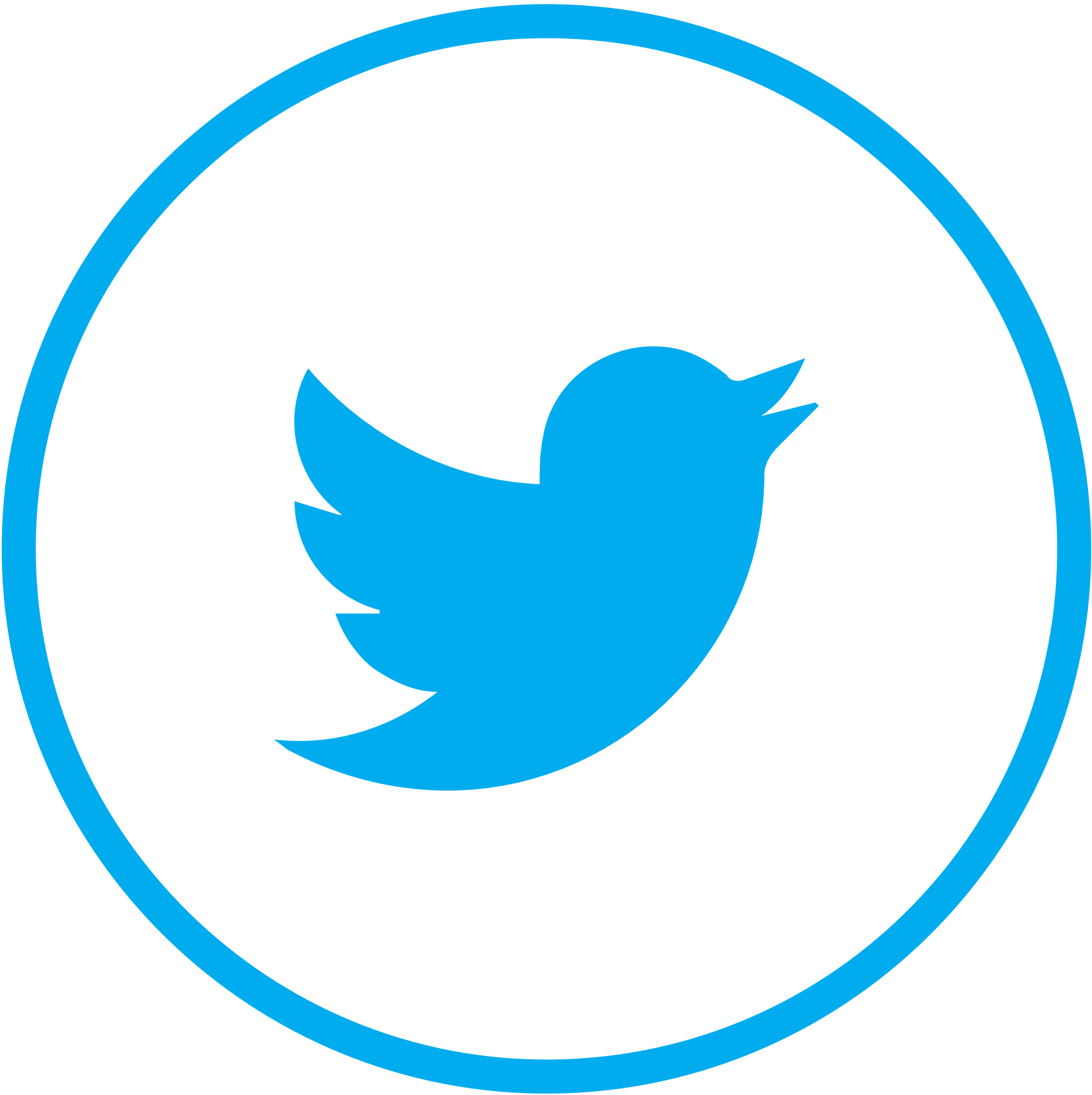
Copied to clipboard

Share





Linkedin



Twitter



Copy Link

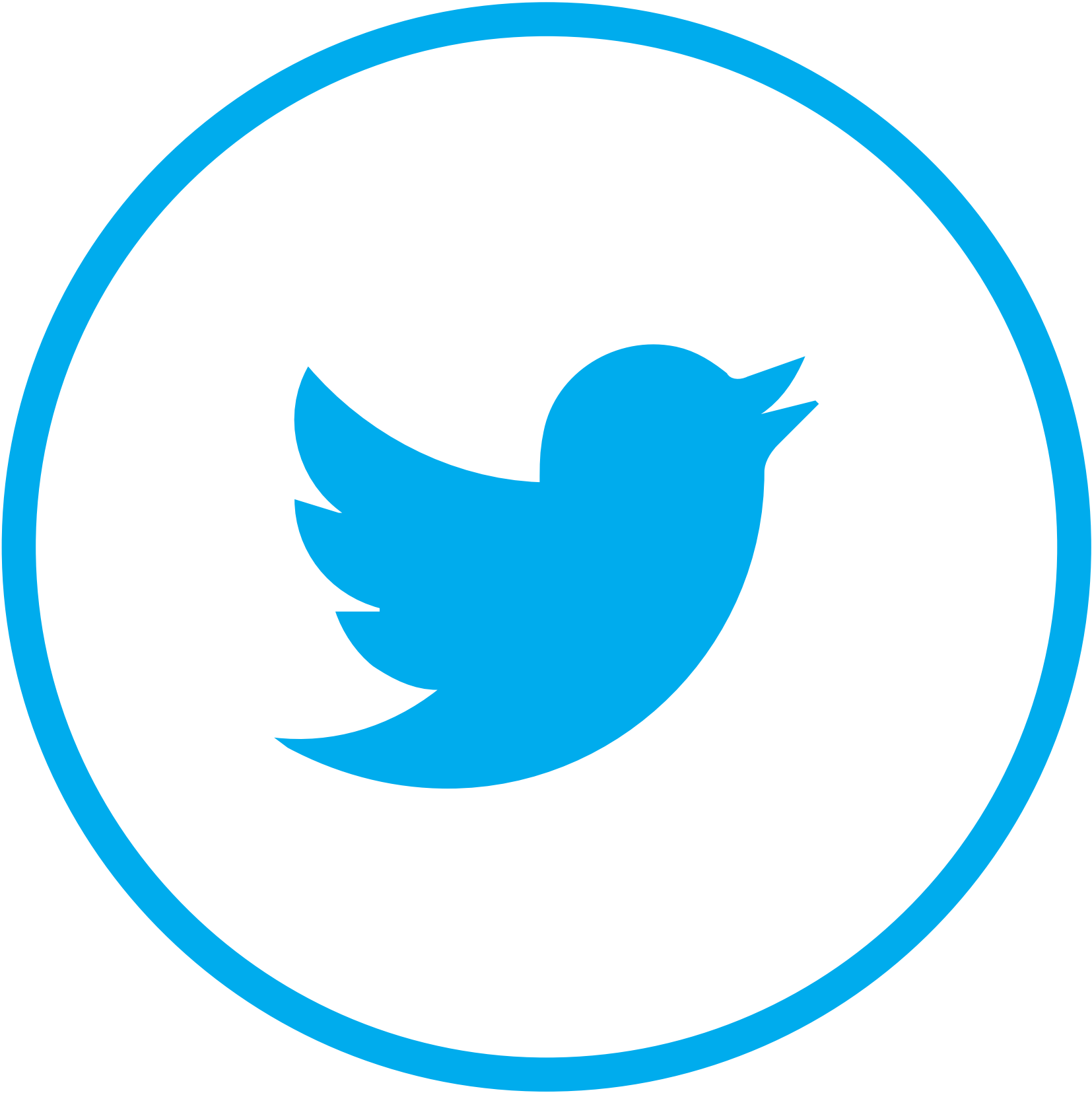


Copied to clipboard

Share







Malware analysis report on SparrowDoor malware

A technical analysis of a new variant of the SparrowDoor malware.Invalid DateTime



The NCSC malware analysis report on a variant of the SparrowDoor malware is available below, along with indicators of compromise, STIX and detection rules.

The report covers technical analysis of a variant of SparrowDoor reported by ESET in September 2021. The variant was found on a UK network in 2021 and contains additional functionality.

SparrowDoor is a persistent loader and backdoor which employs XOR encoding for the C2 channel underneath HTTPS. The additional functionality includes clipboard logging, AV detection, inline hooking of Windows API functions and token impersonation.

Downloads



[Malware Analysis Report SparrowDoor](#)

[This report covers technical analysis of a new variant of the SparrowDoor malware.](#)

- [pdf](#)
- [523 KB](#)



[Malware Analysis Report SparrowDoor Indicators](#)

- [CSV](#)
- [1 KB](#)



[Malware Analysis Report SparrowDoor Sigma](#)

- [• txt](#)
- [• 1 KB](#)



[Malware Analysis Report SparrowDoor STIX2.1](#)

- [• json](#)
- [• 179 KB](#)



[Malware Analysis Report SparrowDoor YARA](#)

- [• txt](#)
- [• 6 KB](#)

Back to top

[Download / Print article PDF](#)

Share



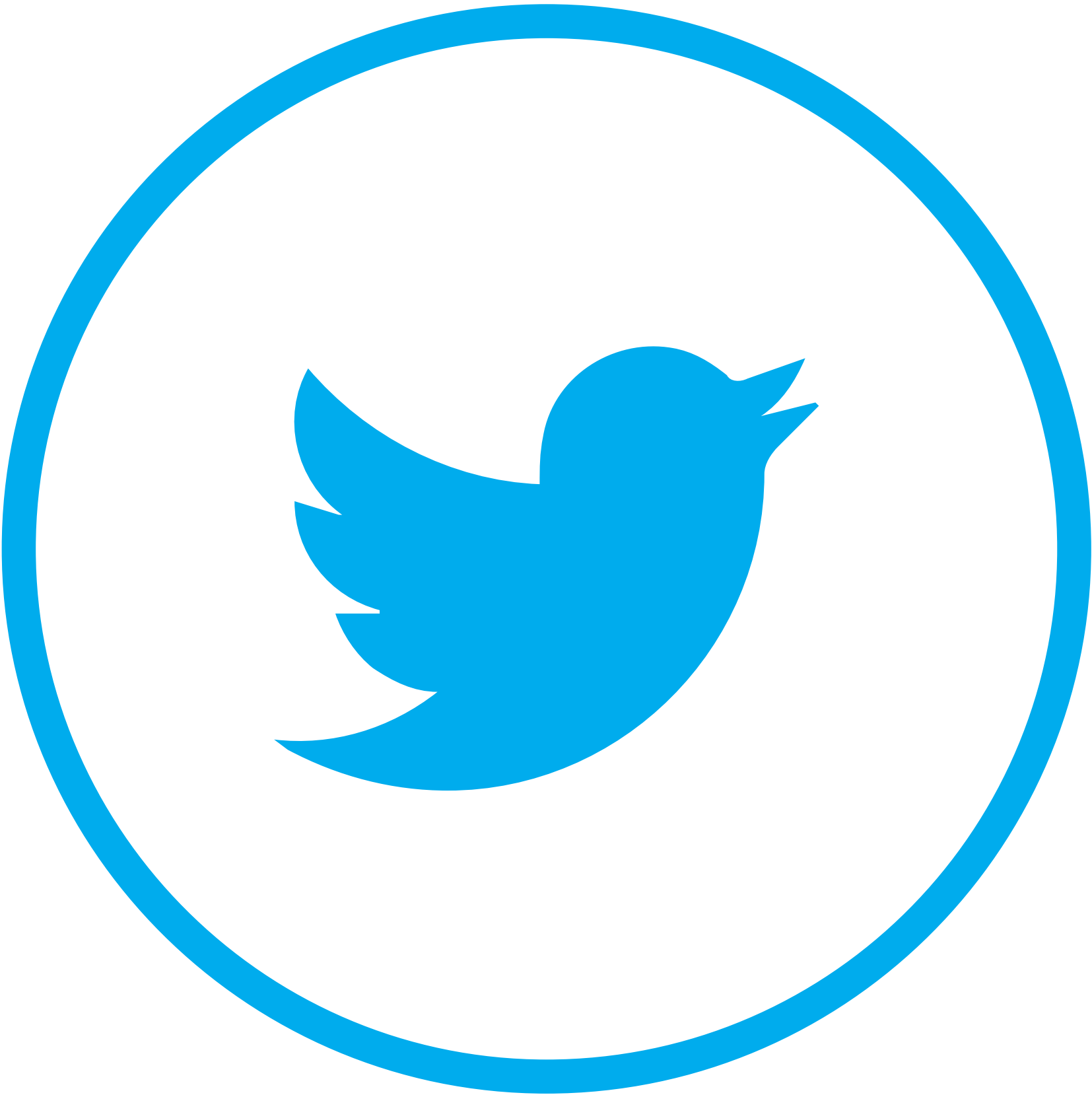
Copied to clipboard

Share





Linkedin



Twitter



Copy Link

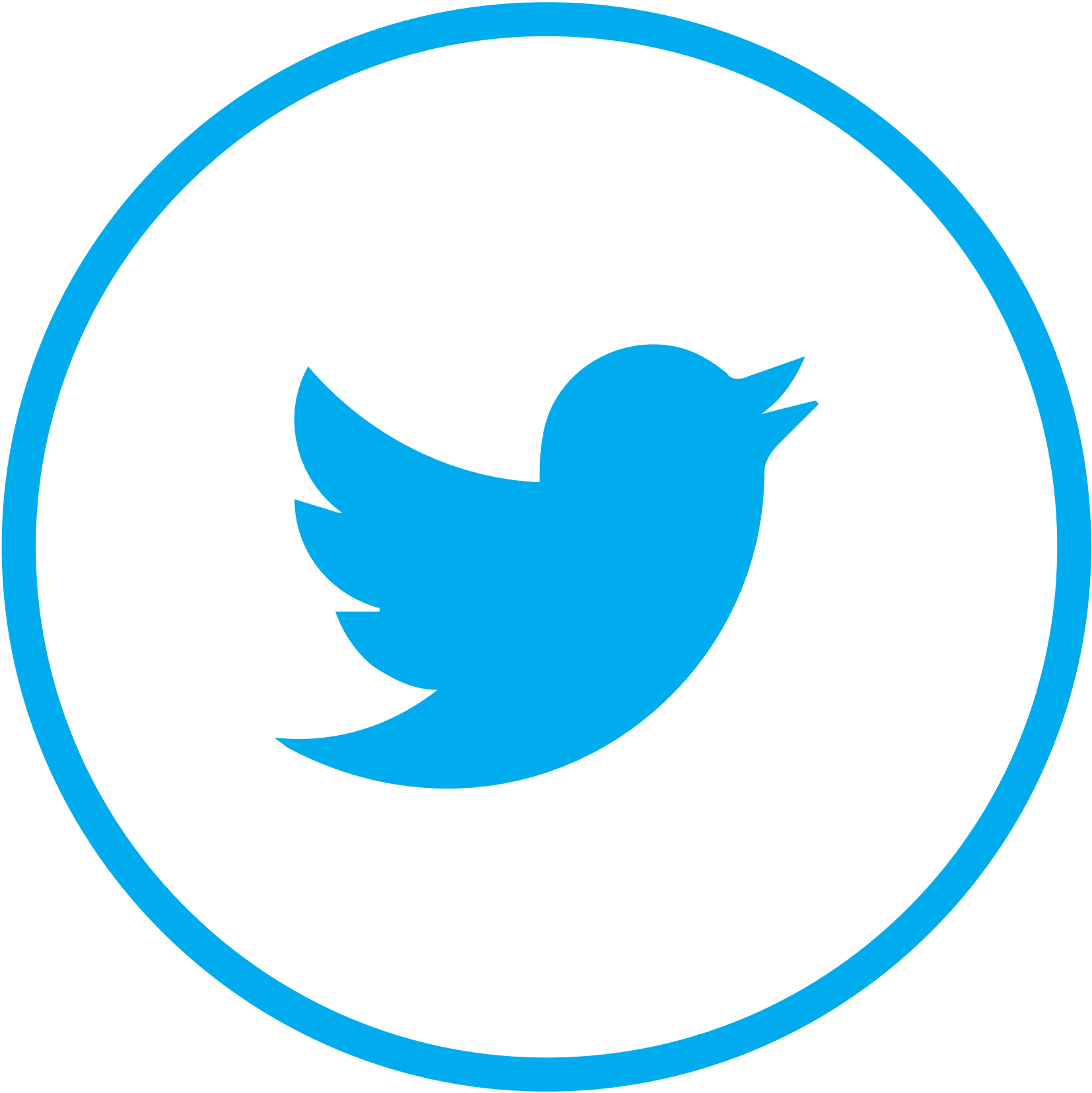


Copied to clipboard

Share







Twitter




Copy Link

• Published

◦ 25 April 2022

• Published

◦ 25 April 2022

 Back to top