# 0558 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:36:31 UTC

## APT group: Storm-0558

| | |
|---|---|
| Names | Storm-0558 *(Microsoft)*<br>Antique Typhoon *(Microsoft)* |
| Country | China |
| Motivation | Information theft and espionage |
| First seen | 2023 |
| Description | (Microsoft) Historically, this threat actor has displayed an interest in targeting media companies, think tanks, and telecommunications equipment and service providers. The objective of most Storm-0558 campaigns is to obtain unauthorized access to email accounts belonging to employees of targeted organizations. Storm-0558 pursues this objective through credential harvesting, phishing campaigns, and OAuth token attacks. This threat actor has displayed an interest in OAuth applications, token theft, and token replay against Microsoft accounts since at least August 2021. Storm-0558 operates with a high degree of technical tradecraft and operational security. The actors are keenly aware of the target's environment, logging policies, authentication requirements, policies, and procedures. Storm-0558's tooling and reconnaissance activity suggests the actor is technically adept, well resourced, and has an in-depth understanding of many authentication techniques and applications.<br><br>While we have discovered some minimal overlaps with other Chinese groups such as Violet Typhoon (APT 31, Judgment Panda, Zirconium), we maintain high confidence that Storm-0558 operates as its own distinct group. |
| Observed | Sectors: Government, Media, Telecommunications, Think Tanks and individuals connected to Taiwan and Uyghur geopolitical interests.<br>Countries: USA and Europe. |
| Tools used | China Chopper. |
| Information | <https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/><br><https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr><br><https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/> |

| | |
|---|---|
| | <https://www.bleepingcomputer.com/news/security/microsoft-breach-led-to-theft-of-60-000-us-state-dept-emails/> |

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format

---

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=23e2ccea-9daa-415a-a72d-b242bbdb3782