Date Posted: 2025/08/04

[Security Alert] Malicious Hijacking of Browser Extensions, Please Strengthen Security Management of Extensions

- Subject: [Security Alert] Malicious Hijacking of Browser Extensions, Please Strengthen Security Management of Extensions
- Content:
  - Forwarded from National Information Security Information Sharing and Analysis Center NISAC-400-202507-00000048
  - The Institute for Information Security observed external cybersecurity intelligence and recently discovered that hackers are conducting malicious hijacking activities targeting browser extensions (such as the Red Direction campaign). The attack method involves implanting malicious code into legitimate extensions during subsequent updates, which can monitor user Browse activity and transmit it to a C2 server, or even redirect to phishing websites. Scope of impact: A total of 18 extensions for Chrome and Edge, potentially affecting over 2.3 million users.
  - Detailed list download link: https://cert.tanet.edu.tw/pdf/2023057048ioc.zip
- Affected Platforms:
  - N/A
- Recommended Action:
  - 1. Inspect and remove all browser extensions confirmed to pose malicious threats.
  - 2. Clear browser cache, cookies, and related session data to prevent ongoing credential leakage risks.
  - 3. Continuously monitor the network behavior of affected hosts and the same network segment to ensure that abnormal activity does not recur.
  - 4. If account credentials are suspected of being leaked, please force a reset of relevant user passwords and multi-factor authentication settings.

Computer and Communications Center
Network Systems Group