Indicators of compromise for malware used by APT28

Published: 2018-10-04 · Archived: 2026-04-02 11:54:21 UTC

Advanced Persistent Threat group, APT28 (also known as Fancy Bear, Pawn Storm, the Sednit Gang and Sofacy), is a highly skilled threat actor. APT28 has previously used tools including X-Tunnel, X-Agent and CompuTrace to penetrate target networks. The signatures and Indicators of Compromise (IoCs) included in this advisory will assist in detecting the presence of APT28 malware on your platforms and networks.

You can download the attached advisory below.

Source: https://www.ncsc.gov.uk/alerts/indicators-compromise-malware-used-apt28