Indicators of compromise for malware used by APT28

This is a technical advisory on the threat actor APT28, written for the network defender community. It provides an overview of the actor and information about associated malware and tooling, with indicators of compromise and signatures that can be used to detect potential presence of the actor on a network. It concludes with mitigation guidelines for protecting networks against activity by APT28 and other hostile actors.

Introduction

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.

PUBLISHED

4 October 2018

WRITTEN FOR

Small & medium sized organisations

Public sector

Large organisations

Cyber security professionals

NEWS TYPE

Alert