LevelBlue - Open Threat Exchange

By mohdrennis

Archived: 2026-04-05 15:53:09 UTC

- Created 7 years ago
- Modified 7 years ago by AlienVault
- Public
- TLP: White

CVE: 2 | **FileHash-MD5:** 8 | **FileHash-SHA256:** 9

Windows zero day was exploited by Buckeye alongside Equation Group tools during 2016 attacks. Exploit and tools continued to be used after Buckeyes apparent disappearance in 2017. The Buckeye attack group was using Equation Group tools to gain persistent access to target organizations at least a year prior to the Shadow Brokers leak.
