Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:32:04 UTC

Description(ESET) On August 27, 2018, a so-called zero-day vulnerability affecting Microsoft Windows was published on GitHub and publicized via a rather acerbic tweet.

It seems obvious that this was not part of a coordinated vulnerability disclosure and there was no patch at the time this tweet (since deleted) was published to fix the vulnerability.

It affects Microsoft Windows OSes from Windows 7 to Windows 10, and in particular the Advanced Local Procedure Call (ALPC) function, and allows a Local Privilege Escalation (LPE). LPE allows an executable or process to escalate privileges. In that specific case, it allows an executable launched by a restricted user to gain administrative rights.

The tweet linked to a GitHub repository that contains Proof-of-Concept code for the exploit. Not only was a compiled version released – the source code was also. Consequently, anyone can modify and recompile the exploit, in order to “improve it”, evade detection, or even incorporate it into their code.

As one could have predicted, it took only two days before we first identified the use of this exploit in a malicious campaign from a group we have dubbed PowerPool. This group has a small number of victims and according to both our telemetry and uploads to VirusTotal (we only considered manual uploads from the web interface), the targeted countries include Chile, Germany, India, the Philippines, Poland, Russia, the United Kingdom, the United States and Ukraine.
