OLDBAIT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:13:56 UTC

According to FireEye, OLDBAIT is a credential stealer that has been observed to be used by APT28.
It targets Internet Explorer, Mozilla Firefox, Eudora, The Bat! (an email client by a Moldovan company), and Becky! (an email client made by a Japanese company). It can use both HTTP or SMTP to exfiltrate data.
In some places it is mistakenly named "Sasfis", which however seems to be a completely different and unrelated malware family.

▶ [TLP:WHITE] win_oldbait_auto (20251219 | Detects win.oldbait.)
