

## Regin (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:33:08 UTC

Regin is a sophisticated malware and hacking toolkit attributed to United States' National Security Agency (NSA) for government spying operations. It was first publicly revealed by Kaspersky Lab, Symantec, and The Intercept in November 2014. Regin malware targeted victims in a range of industries, telecom, government, and financial institutions. It was engineered to be modular and over time dozens of modules have been found and attributed to this family. Symantec observed around 100 infections in 10 different countries across a variety of organisations including private companies, government entities, and research institutes.

► [TLP:WHITE] win\_regin\_auto (20251219 | Detects win.regin.)

---

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.regin>