EvilGnome (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:18:28 UTC

elf.evilgnome (Back to overview)

EvilGnome

Actor(s): Gamaredon Group

According to Infosec Institute, EvilGnome presents itself to unwitting Linux users as a legitimate GNOME extension. Legitimate extensions help to extend Linux functionality, but instead of a healthy boost in system functionality, EvilGnome begins spying on users with an array of functionalities uncommon for most Linux malware types.

References

2024-11-22 · cocomelonc · cocomelonc
Linux malware development 3: linux process injection with ptrace. Simple C example.
EvilGnome HiddenWasp Turla RAT

2021-11-04 · Security Service of Ukraine · Security Service of Ukraine
Gamaredon / Armageddon Group: FSB RF Cyber attacks against Ukraine
EvilGnome Pteranodon RMS

2020-06-16 · Intezer · Aviygayil Mechtinger
ELF Malware Analysis 101: Linux Threats No Longer an Afterthought
Cloud Snooper Dacls EvilGnome HiddenWasp MESSAGETAP NOTROBIN QNAPCrypt Winnti

2019-07-17 · Intezer · Paul Litvak
EvilGnome: Rare Malware Spying on Linux Desktop Users
EvilGnome

There is no Yara-Signature yet.
