

GitHub - telekom-security/malware_analysis: This repository contains analysis scripts, YARA rules, and additional IoCs related to our Telekom Security blog posts.

By lazydaemon

Archived: 2026-04-05 19:41:39 UTC

Folders and files

Name	Name	Last commit message	Last commit date
Latest commit Merge branch 'main' of https://github.com/telekom-security/malware an... Mar 4, 2026 755efb6 · Mar 4, 2026 History 38 Commits			
crylock	crylock	Adds more hashes and the link to the blog post	Jul 14, 2021
darkgate	darkgate	Update extractor.py	Sep 26, 2023
defray777	defray777	Formatting	Mar 18, 2022

Name	Name	Last commit message	Last commit date
flubot	flubot	Adds links for Flubot blog.post	Sep 14, 2021
hacktools	hacktools	fix fp in debian	Dec 12, 2023
icedid	icedid	Merge branch 'patch-3' of https://github.com/Neo23x0/icedid_analysis ...	Jul 8, 2021
iocs	iocs	ivanti cve-2026-1281 iocs	Mar 4, 2026
plugx	plugx	Improved comments a bit.	Oct 29, 2021
raspberrypi_robin	raspberrypi_robin	raspberrypi_robin tweet iocs	Sep 2, 2022
systembc	systembc	Update systembc.yara	Mar 13, 2022
.gitignore	.gitignore	Initial commit	May 7, 2021
README.md	README.md	Update README.md	Sep 8, 2022

- [README](#)

Source: https://github.com/telekom-security/icedid_analysis