Telekom Security Malare Analysis Repository

github.com/telekom-security/icedid_analysis

telekom-security

This repository comprises scripts, signatures, and additional IOCs of our blog posts at the telekom.com blog as well as of our Twitter account.

- 2021-05-17: Let's set ice on fire: Hunting and detecting IcedID infections (IcedID)
- 2021-07-14: LOCKDATA Auction – Another leak marketplace showing the recent shift of ransomware operators (CryLock)
- 2021-09-14: Flubot's Smishing Campaigns under the Microscope (Flubot/Teabot)
- 2021-10-29: #YARA rule for hunting XOR encrypted #PlugX / #Korplug payloads(PlugX)
- 2022-01-14: #100DaysOfYara Detect Hacktools that modify RDP settings (Hacktools)
- 2022-03-11: SystemBC YARA rule and extractor (SystemBC)
- 2022-03-18: #100DaysOfYara Detect Vatet Loader in backedoored Rufus([Defray777]) (https://github.com/telekom-security/malware_analysis/tree/main/defray777)