ioc_signatures/Lazarus_APT37 at main · hvs-consulting/ioc_signatures

By Markus Pölloth

Archived: 2026-04-02 12:08:49 UTC

Lazarus / APT37 IOCs

- Version 1.0
- Date: 15.12.2020
- Author: HvS-Consulting AG

Context

- We used those IOCs in recent investigations to search for traces of 2020s Lazarus / APT37 campaigns.
- More context and matching TTPs can be found in our report: https://www.hvs-consulting.de/media/downloads/ThreatReport-Lazarus.pdf

Notes & Disclaimer

- Most of the given C2 Domains are legit websites, which were hacked and abused by the Lazarus group. If you observe traffic to these domains in your organization, it might also be legit use of these websites. In our report more details about the functionality of the C2 communication are shared, which helps by identifying malicious traffic.
- We provided hashes for many samples, but please note that especially the hashes were changed by the attacker to be different on each system.
- Even if we try to avoid false positives by manual QA, those rules are not meant to be used in production without previous dry runs.
