Ransomware cartography (2014-2024)

Legend:

- 🟧 Threat Group/Author
- ⬛ Ransomware operation/Variant
- ▨ Hack&Leak operation (no encryption)
- → Rebrand/Subset
- - - → Similarities/Relationship
- · · · → Unconfirmed relationship/ Source Code reuse

Author: Marine Pichon
CERT ORANGE CYBERDEFENSE

This graph does not aim at being exhaustive. Its goal is to showcase relationships between relevant ransomware operations and does not purposely list all existing ransomware groups since 2015. Names of strains and associated threat actors were chosen arbitrarily by us among the most popular alias used among the cybersecurity community. It does not mean we endorse the vendor that created the alias.

As a reminder, it is extremely complex to assert relationship and attribution when looking at the cybercrime ecosystem: threat actors are extremely volatile and connected between each other, making effective collaborations hard to define and track over time. In addition to our internal resources (monitoring, reverse engineering, Incident Response engagements related to most of these prominent groups), this mapping makes use of numerous public and private reports from incident responders, malware analysts, CTI researchers,… We paid attention to carefully select, corroborate and fact-check such intelligence with trusted and well recognized sources, but may have still made small mistakes or debatable associations.
Don't hesitate to send us your feedback if any.

Version 26 - 15/03/2024

Cyberdefense