malware-ioc/RagnarLoader at master · prodaft/malware-ioc

By prodaftcatalyst

Archived: 2026-04-05 15:44:50 UTC

Ragnar Loader Indicators of Compromise (IOC)

Ragnar Loader, also known as Sardonic, is a sophisticated toolkit of the Monstrous Mantis (a.k.a. Ragnar Locker) ransomware group, which has been inflicting targeted cyberattacks on organizations since its emergence in 2020. Ragnar Loader often referred to as the Ragnar Framework by its affiliates—plays an essential role by establishing persistent access to compromised systems and ensuring long-term fixation. This loader not only facilitates the initial breach but also lays the groundwork for further network takeover and control.

Original guide and translation of usage for the loader which includes details about the infrastructure can be read from the links.

Report can be found at Catalyst Platform.

Operational Environment

Command and Control Servers

```
 104.238.34.209
173.44.141.47
173.44.141.126
173-44-141-47.nip.io
104-238-34-209.nip.io
```

Hashes

SHA256
9e0611913bdf8493fcae353e3fe78c3d01ae43d8aa1fd92940e84934c31b8729
838ad9a8c49660120ccd52d79b9eeaa43ea62eedaa9ae4c1451fb0edce4978ec
dae284f6383b7b59d92947fb79e556582d9a4f5a860846925713093cb9a874fa

---