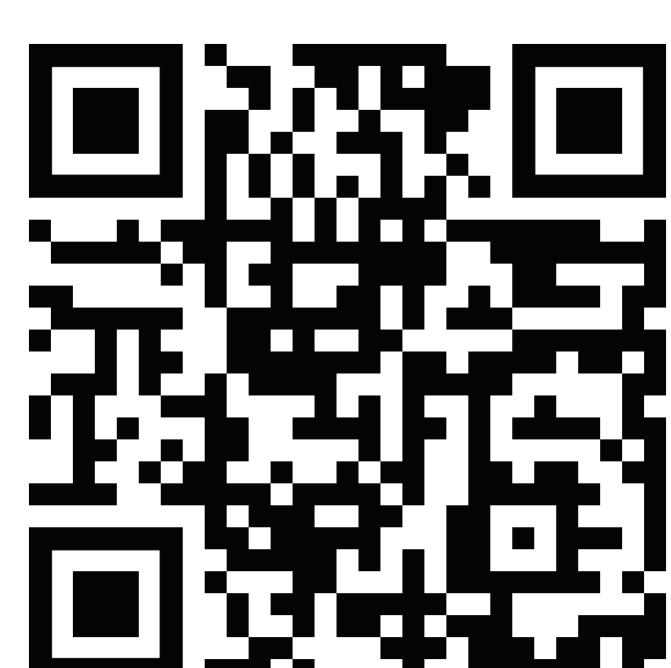


0x00 Sandbox

x86-64 i386 MIPS ARM
Aarch64 PPC64



github.com/danieluhricek/lisa

0x01 Analýza malwaru

Statická analýza

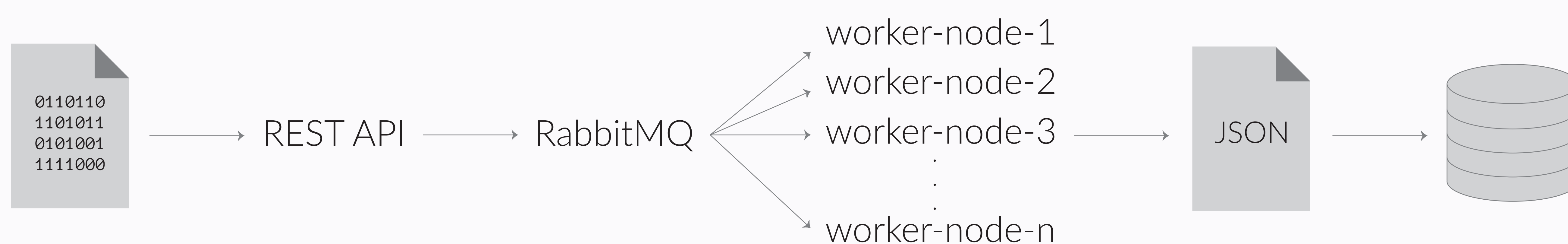
Dynamická analýza

Síťová analýza

VirusTotal modul

plugin systém s definovatelnými moduly

0x02 Architektura



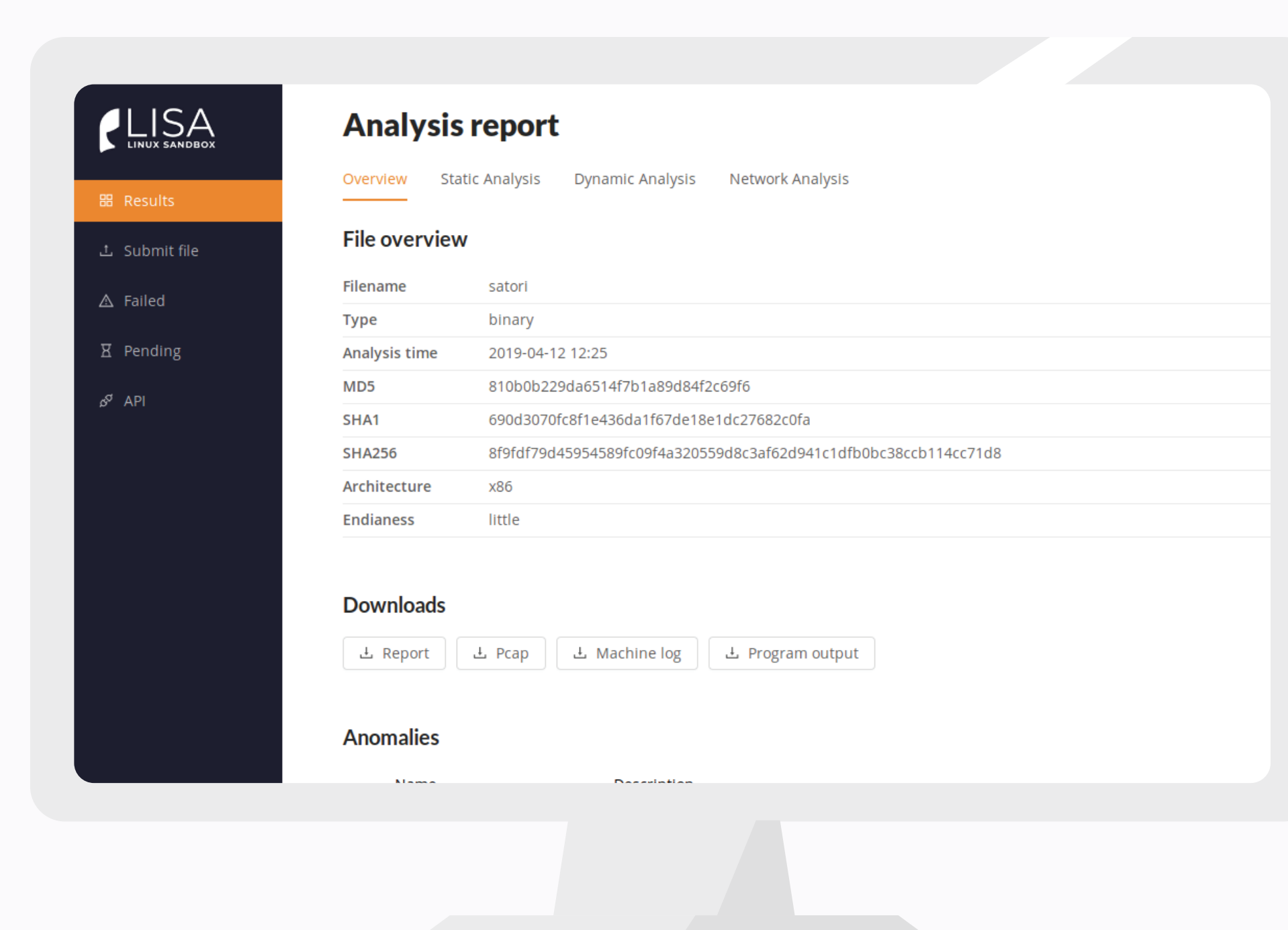
```

import "lisa"

rule blacklisted
{
  condition:
    lisa.network.blacklisted_ip_access()
}

rule syn_scanning
{
  condition:
    lisa.network.syn_scan()
}
  
```

YARA pravidla



frontend

0x03 Technologie

QEMU libpcap Docker Python C++ SystemTap Buildroot celery
RabbitMQ MariaDB YARA Flask ReactJS radare2 VirusTotal