Sentinel LABS

CiGy Ransomware Targets Linux Systems with Plowed Encryption | Decryptor Available

Antonio Cocomazzi, Jim Walter

Executive Summary

- Sentinel One detected ransomware on a server in the Netherlands
  - The ELF executable contains references to the ransom note, encrypted files, and the extension CiGy
  - Linux ransomware is not the most common thing we see on a daily basis
  - Leveraging the ransomware decryptor for the impacted victim

Background

Ransomware is a type of malicious software (malware) that threatens to publish the victim's data or perpetually restrict access to it, unless a ransom is paid to the threat actor. The ransom amount is typically in the thousands of dollars, payable to cyber criminals, often in cryptocurrency, such as Bitcoin, to regain access to the victim's data.

The ransomware ecosystem is ever-changing and ever-evolving. Ransomware-as-a-service (RaaS) is a business model where developers create ransomware and lease it to affiliates, who then carry out the attacks. The RaaS model has fueled the growth of ransomware by lowering the barrier to entry for cybercriminals, allowing even those with limited technical skills to launch sophisticated attacks.

ELF Technical Analysis

Sentinel One detected ransomware on a server in the Netherlands. Upon investigation, we found a Linux ELF (Executable and Linking Format) binary with no AV detections. It appears to be a Go-compiled ransomware sample. The binary uses Go's standard libraries and includes typical ransomware functionality, including file encryption, ransom note generation, and system modification.

The ELF binary is not stripped, which makes reverse engineering easier. The binary includes debug information and function symbols, which helps us understand its structure and functionality. We can see the ransomware's main functions, including encryption routines, ransom note generation, and system modification.

```
$ file -b -p -v -n -m -e elf -e tokens -e cdf -e elf_v0 -e elf_v1 -e elf_v2 -e elf_v3 -e elf_v4 -e elf_v5 -e elf_v6 -e elf_v7 -e elf_v8 -e elf_v9 -e elf_v10 -e elf_v11 -e elf_v12 -e elf_v13 -e elf_v14 -e elf_v15 -e elf_v16 -e elf_v17 -e elf_v18 -e elf_v19 -e
```