Fs0ciety Locker Ransomware Analysis

By Elastio

Published: 2025-07-30 · Archived: 2026-04-05 14:10:09 UTC

Ransomware Research

Fs0ciety Locker is a malicious ransomware strain that encrypts victim files and demands ransom payment for decryption. First observed in the wild on September 1, 2016, this ransomware has been actively targeting systems worldwide.

Quick facts

Ransomware Family

Fs0ciety Locker

First Seen

September 1, 2016

How Fs0ciety Locker ransomware works

File encryption patterns

Fs0ciety Locker modifies encrypted files using specific patterns to mark them as encrypted:

Extensions added after encryption

.realfs0ciety@sigaint.org.fs0ciety

Ransom note and payment demands

After encrypting files, Fs0ciety Locker displays ransom notes demanding payment for file recovery:

filefs0ciety.html

```
notes/fs0ciety.html
```

Location: RansomPayloadStartFolder

Technical indicators

Associated executable files

The following executable files are associated with Fs0ciety Locker ransomware:

- driver_update.exe
- driver_update[1].exe
- Invoice_payment.docm

About this analysis

This Fs0ciety Locker ransomware analysis is part of Elastio's comprehensive ransomware detection database. Elastio provides advanced ransomware protection and recovery, helping organizations defend against and recover from ransomware attacks like Fs0ciety Locker.

Last updated: December 30, 2025

Detection coverage

Elastio detects Fs0ciety Locker inside your data and backups.

The Hunt Engine uses Deep File Inspection to identify Fs0ciety Locker across live data, replicated data, and backups. If this family is in your environment, Elastio finds it before encryption completes. Run a scan against your recovery points to confirm.

Recent ransomware

Explore other threats in our database
