

# GitHub - MDudek-ICS/TRISIS-TRITON-HATMAN: Repository containing original and decompiled files of TRISIS/TRITON/HATMAN malware

By MDudek-ICS

Archived: 2026-04-05 19:04:08 UTC

## TRISIS / TRITON / HatMan Malware Repository

### Description

This repository contains original samples and decompiled sources of malware attacking commonly used in Industrial Control Systems (ICS) *Triconex* Safety Instrumented System (SIS) controllers. For more information scroll to "*Learn More*".

Each organization describing this malware in reports used a different name (TRISIS/TRITON/HatMan). For that reason, there is no one, common name for it.

Folder *original\_samples* contains original files used by the malware that could be found in the wild:

Name	MD5	Contains	MD5
trilog.7z	0b4e76e84fa4d6a9716d89107626da9b	trilog.exe	6c39c3f4a08d3d78f2eb973a94bd7718
library.7z	76f84d3aee53b2856575c9f55a9487e7	library.zip	0face841f7b2953e7c29c064d6886523
imain.7z	d173e8016e73f0f2c17b5217a31153be	imain.bin	437f135ba179959a580412e564d3107f
inject.7z	80fdda5ea7eec98bfdd07fec8f644c2d	inject.bin	0544d425c7555dc4e9d76b571f31f500
all.7z	c382f242f62a3c5f4aab2093f6e0fb2f	All files above	-

All archives are secured with password: *infected*

Folder *decompiled\_code* contains decompiled python files, originating from *trilog.exe* file and *library.zip* archive described above:

Origin	Result	Method
trilog.exe	script_test.py	unpy2exe + uncompile6
library.zip	Files in folder library	uncompile6

Folder *yara\_rules* contains yara rules (that I am aware of) detecting this malware:

File	Author
mandiant.yara	@itsreallynick (Mandiant)
ics-cert.yara	DHS/NCCIC/ICS-CERT
ics-cert-v2.yara	DHS/NCCIC/ICS-CERT ( <a href="#">from update B report</a> )

Folder *symbolic\_execution* contains script for running imain.bin with ANGR symbolic execution engine – credits to [@bl4ckic3](#)

### Why Publishing? Isn't it dangerous?

Some people in the community were raising the issue that publishing the samples and decompiled sources might be dangerous. I agreed until these were not public. I have found the included files in at least two publicly available sources, that means anyone can download it if know where to search. What is more, I believe that organizations/people who could be able to reuse it and have the capability to deploy it in a real attack have already accessed it long time ago. This repository makes it more accessible for community and academia who might work on improving defense solutions and saves some time on looking for decompilers.

### Learn more

#### Technical Analysis:

- [Report by Dragos](#)
- [Report by Mandiant \(FireEye\)](#)
- [Report by ICS-CERT \(NCCIC\)](#)
- [Report by ICS-CERT \(NCCIC\) Update A](#)
- [Report by ICS-CERT \(NCCIC\) Update B](#)
- [Webinar by Dragos \(video\)](#)
- [Analysis by Craftsman Safety Lab \(in Chinese\)](#)
- [Analysis by Midnight Blue](#)
- [Schneider Electric analysis on S4x18 \(video\)](#)
- [Mandiant analysis on S4x18 \(video\)](#)
- [Dragos analysis on S4x18 \(video\)](#)
- [Accenture analysis](#)
- [FireEye analysis of similarities between Triton code and TriStation dlls](#)
- [Dragos presentation from Recon](#)
- [Marina Krotofil and Jos Wetzels presentation from Defcon](#)
- [<- +Marina's reponse regarding plagiarism clamis and nice Triton publications timeline](#)
- [Xenotime TTP by Dragos](#)
- [Triton actor TTP by FireEye](#)
- [Triton incident response story on S4x19 \(video\)](#)

## Attribution

- [Description of a group behind - "Xenotime"](#)
- [Triton attribution by FireEye](#)

## News Publications:

- [Assumption that Aramco was a target](#)
- [Description of analysis and information sharing process](#)
- [How it was leaked to the Internet](#)

## Others:

- [Academic POC attack on Tricon \(published a year ahead\)](#)
- [Defense recommendations](#)
- [Files compilation times](#)
- [ABB security notification](#)

## Detection:

- [Tricotools](#) - A collection of utilities and tools related to the Triconex: TriStation Wireshark dissector and Triconex Honeypot
- [Tristation LUA dissector](#)
- [Triton SNORT rules](#) by BSI

**Any updates to the repository are warmly welcome**

Contact:

- [@dudekmar](#)
- [contact\(at\)marcindudek.com](mailto:contact@marcindudek.com)

---

Source: <https://github.com/ICSrepo/TRISIS-TRITON-HATMAN>